BAB II

LANDASAN TEORI

2.1 Keamanan Informasi dan Sistem Manajemen Keamanan Informasi

2.1.1 Keamanan Informasi

Keamanan informasi merupakan sebuah usaha untuk melindungi aset informasi yang terdapat pada perusahaan dari segala ancaman yang dapat saja terjadi [15]. Keamanan informasi memiliki tujuan untuk mencapai tiga tujuan utama, yang terdiri dari aspek kerahasiaan, integritas, dan ketersediaan informasi [16].

Gambar 2.1 Aspek Keamanan Informasi

- Kerahasiaan *(confidentiality)*: informasi tidak dapat diakses oleh pihak-pihak yang tidak memiliki otoritas dan hanya dapat diakses oleh pihak-pihak yang berwenang atau memiliki otoritas.
- Integritas *(integrity)*: informasi hanya dapat dimodifikasi atau diubah oleh pihak-pihak yang berwenang atau memiliki otoritas serta menjaga akurasi data.
- Ketersediaan *(availability)*: informasi tersedia atau dapat diakses ketika dibutuhkan oleh pihak-pihak yang memiliki otoritas [17].

Keamanan informasi juga bertujuan untuk mencegah adanya kerusakan dan kehilangan informasi serta tersebarnya informasi kepada pihak yang tidak bertanggung jawab [16]. Keamanan informasi juga memiliki tujuan untuk menjaga keberlanjutan bisnis sebuah perusahaan dan meminimalisir penurunan

nilai bisnis yang diakibatkan oleh efek dari insiden atau ancaman yang terjadi [18]. Oleh karena itu, perusahaan harus selalu mengedepankan dan meningkatkan keamanan informasi guna melindungi perusahaan dari potensi ancaman yang dapat mengancam keberlangsungan bisnis perusahaan.

2.1.2 SMKI (Sistem Manajemen Keamanan Informasi)

SMKI (Sistem manajemen keamanan informasi) merupakan proses yang telah dirancang dengan berdasarkan *plan* (perencanaan), *do* (implementasi), *check* (evaluasi), dan *act* (meningkatkan) terhadap keamanan informasi yang terdapat pada perusahaan. Sistem manajemen keamanan informasi bertujuan untuk meminimalisir adanya ancaman-ancaman yang muncul terhadap keamanan informasi [19]. Selain itu, adanya sistem manajemen keamanan informasi juga dapat memberikan pengamanan informasi yang lebih kuat sehingga informasi perusahaan dapat terjaga dari pihak-pihak yang tidak bertanggung jawab.

Adanya Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi menunjukkan bahwa informasi merupakan aset penting dan perlu adanya pengamanan yang kuat terhadap informasi tersebut. Sistem manajemen keamanan informasi pada perusahaan perlu untuk dievaluasi secara berkala sehingga perusahaan dapat menemukan celah-celah yang kemungkinan dapat menyebabkan timbulnya ancaman terhadap keamanan informasi [20].

2.2 ISO 27001:2013

ISO (*International Standardization Organization*) merupakan suatu badan internasional yang bertugas menciptakan dan menerbitkan standar-standar yang akan diberlakukan untuk seluruh dunia. Saat ini, ISO telah menerbitkan standar internasional sebanyak 24.674 dan standar-standar tersebut telah mencakup hampir seluruh aspek teknologi, manajemen, dan manufaktur [21]. Salah satu standar internasional yang diterbitkan oleh ISO adalah ISO 27001:2013. ISO 27001:2013 merupakan standar internasional yang digunakan sebagai pedoman dalam penerapan sistem manajemen keamanan informasi atau *information security*

management systems (ISMS). Tujuan utama dari ISO 27001:2013 adalah memastikan kerahasiaan, integritas, dan ketersediaan informasi.

Pada ISO 27001:2013 terdapat 11 klausul yang merupakan persyaratan inti dalam standar ISO 27001. Klausul-klausul tersebut, antara lain:

1. 0 – *Introduction*
2. 1 – *Scope*
3. 2 – *Normative references*
4. 3 – *Terms and definitions*
5. 4 – *Context of the organization*
6. 5 – *Leadership*
7. 6 – *Planning*
8. 7 – *Support*
9. 8 – *Operation*
10. 9 – *Performance Evaluation*
11. 10 - *Improvement*

Selain klausul, terdapat juga 14 kontrol pada *Annex A* di ISO 27001:2013. Berikut adalah *Annex A* yang terdapat dalam standar ISO 27001:2013:

1. *Information security policies* (Kebijakan Keamanan Informasi)
   Annex A ini membahas mengenai kebijakan keamanan informasi dan peninjauan kebijakan keamanan informasi.
2. *Organization of information security* (Organisasi Keamanan Informasi)
   Annex A ini membahas mengenai tanggung jawab dan peran dalam keamanan informasi, pemisahan tugas, komunikasi dengan pihak berwenang, komunikasi dengan kelompok minat khusus, keamanan informasi dalam *project management*, kebijakan perangkat seluler, dan *teleworking*.
3. *Human resource security* (Keamanan Sumber Daya Manusia)
   Annex A ini membahas mengenai *screening*, ketentuan dan kondisi kerja, tanggung jawab manajemen, kesadaran, edukasi dan pelatihan keamanan

informasi, proses pendisiplinan, dan pemutusan atau perubahan tanggung jawab pekerjaan.

4. *Asset management* (Manajemen Aset)

   Annex A ini membahas mengenai inventaris aset, kepemilikan aset, penggunaan aset, pengembalian aset, klasifikasi informasi, pelabelan informasi, penanganan aset, manajemen media yang dapat dipindahkan, pembuangan media, dan transfer media fisik.

5. *Access control* (Akses Kontrol)

   Annex A ini membahas mengenai kebijakan kontrol akses, akses ke jaringan dan layanan jaringan, registrasi dan de-registrasi pengguna, penyediaan akses pengguna, pengelolaan hak akses istimewa, manajemen informasi otentikasi rahasia pengguna, tinjau hak akses pengguna, pemindahan atau penyesuaian hak akses, penggunaan informasi otentikasi rahasia, pembatasan akses informasi, prosedur *log-on* yang aman, manajemen kata sandi sistem, penggunaan program utilitas istimewa, dan kontrol akses ke *source code* program.

6. *Cryptography* (Kriptografi)

   Annex A ini membahas mengenai kebijakan yang berkaitan dengan penggunaan kontrol kriptografi dan manajemen kunci.

7. *Physical and environmental security* (Keamanan Fisik dan Lingkungan)

   Annex A ini membahas mengenai perimeter keamanan fisik, kontrol entri fisik, pengamanan kantor, kamar dan fasilitas, perlindungan dari ancaman eksternal dan lingkungan, kerja di area yang aman, area pengiriman dan pemuatan, penempatan dan perlindungan peralatan, utilitas pendukung, keamanan kabel, *maintenance* peralatan, pemindahan aset, keamanan peralatan dan aset diluar lokasi, pembuangan yang aman atau penggunaan kembali peralatan, peralatan pengguna tanpa pengawasan, dan kebijakan *clear desk* dan *clear screen.*

8. *Operations security* (Keamanan Operasi)

   Annex A ini membahas mengenai prosedur operasi yang terdokumentasi, manajemen perubahan, manajemen kapasitas, pemisahan lingkungan pengembangan, pengujian dan operasional, kontrol terhadap *malware*, *backup*

informasi, *event logging*, perlindungan informasi *log*, *log* administrator dan operator, sinkronisasi jam, pemasangan perangkat lunak pada sistem operasional, manajemen kerentanan teknis, pembatasan instalasi perangkat lunak, dan kontrol audit sistem informasi.

9. *Communications security* (Keamanan Komunikasi)

   Annex A ini membahas mengenai kontrol jaringan, keamanan layanan jaringan, segregasi dalam jaringan, kebijakan dan prosedur transfer informasi, perjanjian mengenai transfer informasi, *electronic messaging*, dan kerahasiaan atau perjanjian non-pengungkapan.

10. *System acquisition, development and maintenance* (Akuisisi, Pengembangan dan Pemeliharaan Sistem)

    Annex A ini membahas mengenai analisis dan spesifikasi persyaratan keamanan informasi, pengamanan layanan aplikasi di jaringan public, perlindungan transaksi pada layanan aplikasi, kebijakan pengembangan yang aman, prosedur kontrol perubahan sistem, *review* teknis pada aplikasi setelah perubahan *platform* operasi, pembatasan pada perubahan paket perangkat lunak, prinsip-prinsip rekayasa sistem yang aman, lingkungan pengembangan yang aman, pengembangan sumber daya, sistem pengujian keamanan, sistem *acceptance testing*, dan perlindungan terhadap data yang diuji.

11. *Supplier relationships* (Hubungan Pemasok)

    Annex A ini membahas mengenai kebijakan keamanan informasi untuk hubungan pemasok, mengatasi keamanan dalam perjajian pemasok, *supply chain* teknologi informasi dan komunikasi, pemantauan dan peninjauan layanan pemasok, dan mengelola perubahan pada layanan pemasok.

12. *Information security incident management* (Manajemen Insiden Keamanan Informasi)

    Annex A ini membahas mengenai tanggung jawab dan prosedur, pelaporan kejadian keamanan informasi, pelaporan kelemahan keamanan informasi, penilaian dan keputusan tentang peristiwa keamanan informasi, tanggapan insiden keamanan informasi, belajar dari insiden keamanan informasi, dan pengumpulan bukti.

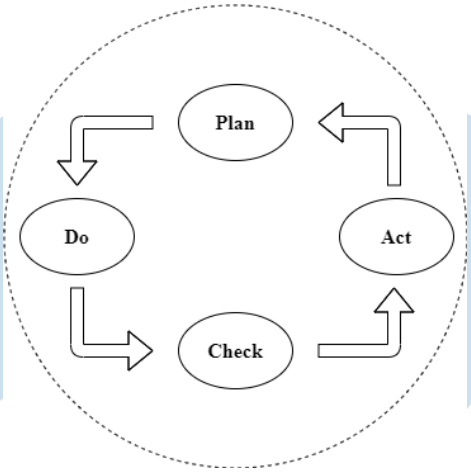
13. *Information security aspects of business continuity management* (Aspek Keamanan Informasi Manajemen Kesinambungan Bisnis)

    Annex A ini membahas mengenai perencanaan kesinambungan keamanan informasi, penerapan kesinambungan keamanan informasi, memeriksa, meninjau dan mengevaluasi kontinuitas keamanan informasi, dan ketersediaan fasilitas pemrosesan informasi.

14. *Compliance* (Kepatuhan)

    Annex A ini membahas mengenai peraturan perundang-undangan dan persyaratan kontrak yang berlaku, hak kekayaan intelektual, perlindungan catatan, privasi dan perlindungan informasi yang dapat diidentifikasi secara pribadi, regulasi kontrol kriptografi, tinjauan independen keamanan informasi, kepatuhan terhadap kebijakan dan standar keamanan, dan tinjauan kepatuhan teknis [22].

Terdapat metode yang telah didefinisikan pada ISO 27001, yaitu siklus atau metode PDCA (*Plan-Do-Check-Act*). Berikut adalah proses atau tahapan-tahapan yang terdapat pada metode PDCA [23]:



Gambar 2.2 Metode PDCA (*Plan-Do-Check-Act*)

- *Plan*

  Tahap ini merupakan tahap merencanakan dan merancang SMKI (Sistem Manajemen Keamanan Informasi), seperti membuat komitmen, kebijakan, kontrol, prosedur, instruksi kerja, dan lain-lain guna memenuhi kebutuhan dan keinginan perusahaan.

- *Do*

  Tahap ini merupakan tahap mengimplementasikan dan mengoperasikan kebijakan, kontrol, dan prosedur yang telah direncanakan pada tahap sebelumnya, yaitu tahap *plan.*
- *Check*

  Tahap ini merupakan tahap pemantauan terhadap pelaksanaan SMKI. Selain itu, terdapat juga evaluasi dan audit terhadap SMKI.
- *Act*

  Tahap ini merupakan tahap pengembangan sehingga akan dilakukan tindakan atau kegiatan yang dapat memperbaiki dan meningkatkan SMKI berdasarkan hasil evaluasi yang diperoleh.

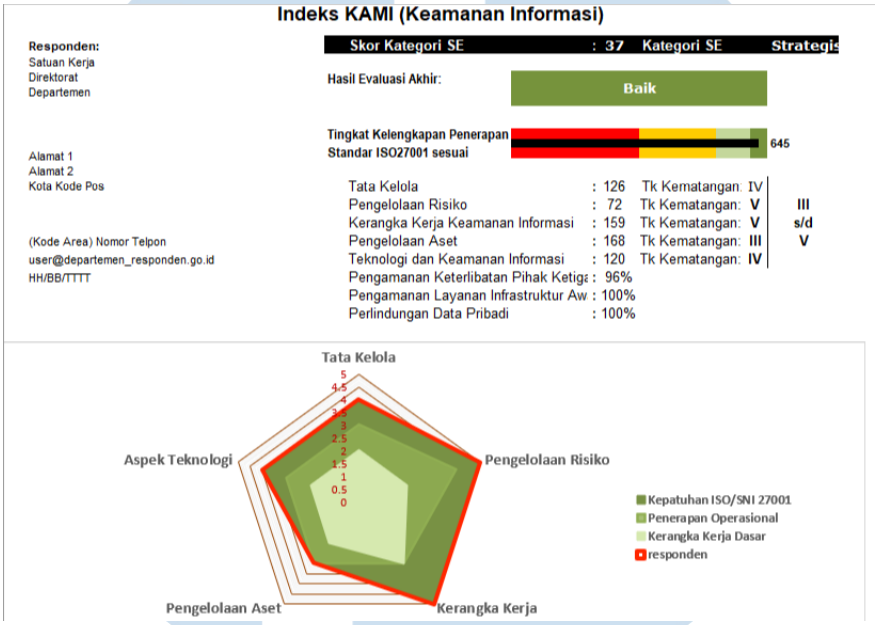
Pada ISO 27001 versi sebelumnya, metode PDCA merupakan proses yang diperlukan untuk menerapkan SMKI. Hal ini dengan jelas terdapat pada klausul 0.2 yang menyatakan bahwa proses yang diperlukan untuk menerapkan SMKI adalah PDCA. Pada ISO 27001:2013 tidak wajib menggunakan metode PDCA, namun metode PDCA masih tetap merupakan proses yang valid dan efektif untuk mengimplementasikan SMKI. Meskipun tidak ada proses yang ditentukan pada ISO 27001:2013, menerapkan PDCA merupakan keputusan yang logis karena telah terbukti sebagai pendekatan praktis selama bertahun-tahun [24].

2.3 Indeks KAMI (Keamanan Informasi)

BSN (Badan Standardisasi Nasional) menetapkan ISO 27001 sebagai standar nasional yang berfokus terhadap teknologi informasi, teknik keamanan, dan sistem manajemen keamanan informasi. Untuk mendapatkan ukuran yang terstandarisasi SNI tersebut, Badan Siber dan Sandi Negara (BSSN) mengeluarkan alat bantu yang dapat digunakan untuk mengevaluasi tingkat kematangan atau kepatuhan dalam penerapan ISO 27001 [7].

Alat bantu tersebut adalah indeks KAMI (Keamanan Informasi). Alat bantu ini dirilis pada tahun 2009 dengan versi 1.0, yang kemudian diperbaharui atau direvisi hingga mencapai versi 4.2. Untuk menggunakan indeks KAMI (Keamanan Informasi), responden harus menjawab pertanyaan-pertanyaan yang telah

disediakan dengan jujur dan sesuai dengan kondisi perusahaan. Hal ini bertujuan agar *dashboard* indeks KAMI (Keamanan Informasi) menampilkan hasil yang valid.



Gambar 2.3 *Dashboard* Indeks KAMI (Keamanan Informasi)
Sumber: Indeks KAMI 4.2

Dashboard di atas akan menampilkan tingkat kepatuhan atau kelengkapan penerapan ISO 27001 serta tingkat kematangan keamanan informasi berdasarkan jawaban yang telah diberikan oleh responden. Adapun tingkat kematangan tersebut terdiri dari:

- Tingkat I: Kondisi Awal
  a. Mulai adanya pemahaman mengenai perlunya pengelolaan keamanan informasi.
  b. 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.
  c. Kelemahan teknis dan non-teknis tidak teridentifikasi dengan baik.
  d. Pihak yang terlibat tidak menyadari tanggung jawab mereka.
- Tingkat II: Penerapan Kerangka Kerja Dasar

a. Pengamanan sudah diterapkan walaupun sebagian besar masih di area teknis dan belum adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif.
b. Proses pengamanan berjalan tanpa dokumentasi atau rekaman resmi.
c. Langkah pengamanan operasional yang diterapkan bergantung kepada pengetahuan dan motivasi individu pelaksana.
d. Bentuk pengamanan secara keseluruhan belum dapat dibuktikan efektivitasnya.
e. Kelemahan dalam manajemen pengamanan masih banyak ditemukan dan tidak dapat diselesaikan dengan tuntas oleh pelaksana maupun pimpinan sehingga menyebabkan dampak yang sangat signifikan.
f. Manajemen pengamanan belum mendapatkan prioritas dan tidak berjalan secara konsisten.
g. Pihak yang terlibat kemungkinan besar masih belum memahami tanggung jawab mereka.

- Tingkat III: Terdefinisi dan Konsisten
  a. Bentuk pengamanan yang baku sudah diterapkan secara konsisten dan terdokumentasi secara resmi.
  b. Efektivitas pengamanan dievaluasi secara berkala, walaupun belum melalui proses yang terstruktur.
  c. 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.
  d. Kerangka kerja pengamanan sudah mematuhi ambang batas minimum standar atau persyaratan hukum yang terkait.
  e. Secara umum semua pihak yang terlibat menyadari tanggungjawab mereka dalam pengamanan informasi.
- Tingkat IV: Terkelola dan Terukur
  a. Pengamanan diterapkan secara efektif sesuai dengan strategi manajemen risiko.

b. Evaluasi (pengukuran) pencapaian sasaran pengaman dilakukan secara rutin, formal dan terdokumentasi.
c. Penerapan pengamanan teknis secara konsisten dievaluasi efektivitasnya.
d. Kelemahan manajemen pengamanan teridentifikasi dengan baik dan secara konsisten ditindaklanjuti pembenahannya.
e. Manajemen pengamanan bersifat pro-aktif dan menerapkan pembenahan untuk mencapai bentuk pengelolaan yang efisien.
f. Insiden dan ketidakpatuhan (non-conformity) diselesaikan melalui proses formal dengan pembelajaran akar permasalahan.
g. Karyawan merupakan bagian yang tidak terpisahkan dari pelaksana pengamanan informasi.

- Tingkat V: Optimal
  a. Pengamanan menyeluruh diterapkan secara berkelanjutan dan efektif melalui program pengelolaan risiko yang terstruktur.
  b. Pengamanan informasi dan manajemen risiko sudah terintegrasi dengan tugas pokok instansi.
  c. Kinerja pengamanan dievaluasi secara kontinyu, dengan analisis parameter efektivitas kontrol, kajian akar permasalahan dan penerapan langkah untuk optimasi peningkatan kinerja.
  d. Target pencapaian program pengamanan informasi selalu dipantau, dievaluasi dan diperbaiki.
  e. Karyawan secara proaktif terlibat dalam peningkatan efektivitas pengamanan [25].

Terdapat lima area dalam indeks KAMI (Keamanan Informasi), yaitu:

- Tata Kelola Keamanan Informasi

  Area ini dirancang untuk mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/perusahaan/fungsi, tugas dan tanggung jawab pengelola keamanan informasi. Berikut tampilan pada area tata kelola keamanan informasi:

Bagian II: Tata Kelola Keamanan Informasi					
Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/perusahaan/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				Status	Skor
#			Fungsi/Organisasi Keamanan Informasi		
2.1	II	1	Apakah pimpinan instansi/perusahaan anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	Diterapkan Secara Menyeluruh	3
2.2	II	1	Apakah instansi/perusahaan anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	Diterapkan Secara Menyeluruh	3
2.3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	Diterapkan Secara Menyeluruh	3
2.4	II	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	Diterapkan Secara Menyeluruh	3
2.5	II	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	Diterapkan Secara Menyeluruh	3
2.6	II	1	Apakah instansi/perusahaan anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	Diterapkan Secara Menyeluruh	3
2.7	II	1	Apakah semua pelaksana pengamanan informasi di instansi/perusahaan anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	Diterapkan Secara Menyeluruh	3
2.8	II	1	Apakah instansi/perusahaan anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	Diterapkan Secara Menyeluruh	3
2.9	II	2	Apakah instansi/perusahaan anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	Diterapkan Secara Menyeluruh	6
2.10	II	2	Apakah instansi/perusahaan anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	Diterapkan Secara Menyeluruh	6

Gambar 2.4 Tampilan Area Tata Kelola Keamanan Informasi
Sumber: Indeks KAMI 4.2

Total jumlah pertanyaan yang ada di area ini adalah sebanyak 22 pertanyaan dan terbagi menjadi 3 tahap. Jumlah pertanyaan pada tahap 1 adalah sebanyak 8 pertanyaan, jumlah pertanyaan pada tahap 2 adalah sebanyak 8 pertanyaan, dan jumlah pertanyaan pada tahap 3 adalah sebanyak 6 pertanyaan. Kategori penilaian pada area ini terdiri dari “Tidak dilakukan”, “Dalam Perencanaan”, “Dalam Penerapan atau Diterapkan Sebagian”, dan “Diterapkan Secara Menyeluruh”.

- Pengelolaan Risiko Keamanan Informasi

Area ini dirancang untuk mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi. Berikut adalah tampilan pada area pengelolaan risiko keamanan informasi:

Bagian III: Pengelolaan Risiko Keamanan Informasi				
Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.				
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			Status	Skor
3.2	II	1	Apakah instansi/perusahaan anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?	Diterapkan Secara Menyeluruh	3
3.3	II	1	Apakah instansi/perusahaan anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Diterapkan Secara Menyeluruh	3
3.4	II	1	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/perusahaan anda?	Diterapkan Secara Menyeluruh	3
3.5	II	1	Apakah instansi/perusahaan anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	Diterapkan Secara Menyeluruh	3
3.6	II	1	Apakah instansi/perusahaan anda sudah mendefinisikan kepemilikan dan pihak pengelola *(custodian)* aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?	Diterapkan Secara Menyeluruh	3
3.7	II	1	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	Diterapkan Secara Menyeluruh	3
3.8	II	1	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	Diterapkan Secara Menyeluruh	3
3.9	II	1	Apakah instansi/perusahaan 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)?	Diterapkan Secara Menyeluruh	3
3.10	II	1	Apakah instansi/perusahaan anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang	Diterapkan Secara Menyeluruh	3

Gambar 2.5 Tampilan Area Pengelolaan Risiko Keamanan Informasi
Sumber: Indeks KAMI 4.2

Total jumlah pertanyaan yang ada di area ini adalah sebanyak 16 pertanyaan dan terbagi menjadi 3 tahap. Jumlah pertanyaan pada tahap 1 adalah sebanyak 10 pertanyaan, jumlah pertanyaan pada tahap 2 adalah sebanyak 4 pertanyaan, dan jumlah pertanyaan pada tahap 3 adalah sebanyak 2 pertanyaan. Kategori penilaian pada area ini terdiri dari "Tidak dilakukan", "Dalam Perencanaan", "Dalam Penerapan atau Diterapkan Sebagian", dan "Diterapkan Secara Menyeluruh".

- Kerangka Kerja Pengelolaan Keamanan Informasi

Area ini dirancang untuk mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya. Berikut adalah tampilan pada area kerangka kerja pengelolaan keamanan informasi:

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi					
Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#			**Penyusunan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi**		
4.1	II	1	Apakah kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggung jawab pihak-pihak yang diberikan wewenang untuk menerapkannya?	Diterapkan Secara Menyeluruh	3
4.2	II	1	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?	Diterapkan Secara Menyeluruh	3
4.3	II	1	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?	Diterapkan Secara Menyeluruh	3
4.4	II	1	Apakah tersedia proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?	Diterapkan Secara Menyeluruh	3
4.5	II	1	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/perusahaan?	Diterapkan Secara Menyeluruh	3
4.6	II	1	Apakah tersedia proses untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan?	Diterapkan Secara Menyeluruh	3
4.7	II	1	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?	Diterapkan Secara Menyeluruh	3

Gambar 2.6 Tampilan Area Kerangka Kerja Pengelolaan Keamanan Informasi
Sumber: Indeks KAMI 4.2

Total jumlah pertanyaan yang ada di area ini adalah sebanyak 29 pertanyaan dan terbagi menjadi 3 tahap. Jumlah pertanyaan pada tahap 1 adalah sebanyak 12 pertanyaan, jumlah pertanyaan pada tahap 2 adalah sebanyak 10 pertanyaan, dan jumlah pertanyaan pada tahap 3 adalah sebanyak 7 pertanyaan. Kategori penilaian pada area ini terdiri dari "Tidak dilakukan", "Dalam Perencanaan", "Dalam Penerapan atau Diterapkan Sebagian", dan "Diterapkan Secara Menyeluruh".

- Pengelolaan Aset Informasi

Area ini dirancang untuk mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut. Berikut adalah tampilan pada area pengelolaan aset informasi:

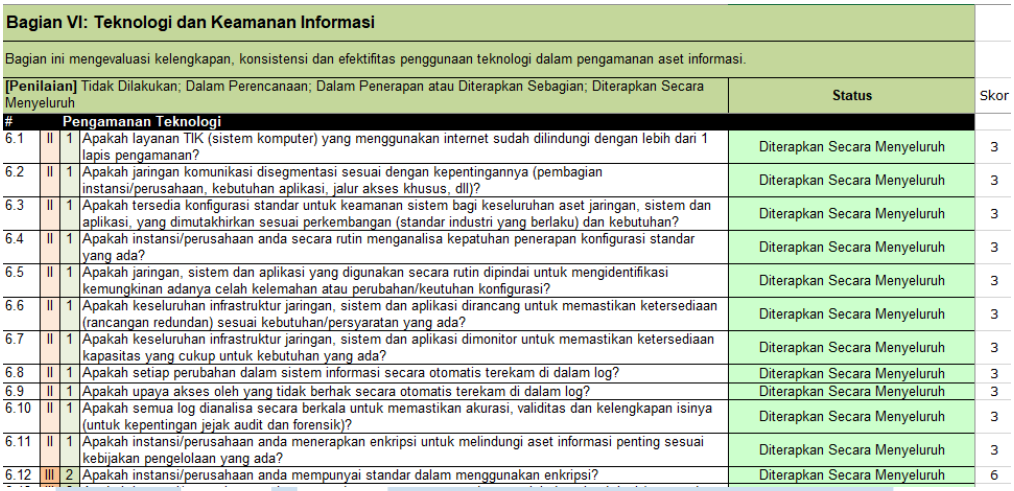
Bagian V: Pengelolaan Aset Informasi					
Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#			**Pengelolaan Aset Informasi**		
5.1	II	1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpelihara ? (termasuk kepemilikan aset)	Diterapkan Secara Menyeluruh	3
5.2	II	1	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?	Diterapkan Secara Menyeluruh	3
5.3	II	1	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi/perusahaan dan keperluan pengamanannya?	Diterapkan Secara Menyeluruh	3
5.4	II	1	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut	Diterapkan Secara Menyeluruh	3
5.5	II	1	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?	Diterapkan Secara Menyeluruh	3
5.6	II	1	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	Diterapkan Secara Menyeluruh	3
5.7	II	1	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	Diterapkan Secara Menyeluruh	3
			Apakah instansi/perusahaan anda memiliki dan menerapkan kontrol keamanan di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?		
5.8	II	1	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di instansi/perusahaan anda	Diterapkan Secara Menyeluruh	3
5.9	II	1	Tata tertib penggunaan komputer, email, internet dan intranet	Diterapkan Secara Menyeluruh	3
5.10	II	1	Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI	Diterapkan Secara Menyeluruh	3

Gambar 2.7 Tampilan Area Pengelolaan Aset Informasi
Sumber: Indeks KAMI 4.2

Total jumlah pertanyaan yang ada di area ini adalah sebanyak 38 pertanyaan dan terbagi menjadi 3 tahap. Jumlah pertanyaan yang terdapat pada tahap 1 adalah sebanyak 24 pertanyaan, jumlah pertanyaan yang terdapat pada tahap 2 adalah sebanyak 10 pertanyaan, dan jumlah pertanyaan yang terdapat pada tahap 3 adalah sebanyak 4 pertanyaan. Kategori penilaian pada area ini terdiri dari “Tidak dilakukan”, “Dalam Perencanaan”, “Dalam Penerapan atau Diterapkan Sebagian”, dan “Diterapkan Secara Menyeluruh”.

- Teknologi dan Keamanan Informasi

Area ini dirancang untuk mengevaluasi kelengkapan, konsistensi, dan efektifitas penggunaan teknologi dalam pengamanan aset informasi. Berikut adalah tampilan pada area teknologi dan keamanan informasi:



Bagian VI: Teknologi dan Keamanan Informasi

Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#			**Pengamanan Teknologi**		
6.1	II	1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	Diterapkan Secara Menyeluruh	3
6.2	II	1	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?	Diterapkan Secara Menyeluruh	3
6.3	II	1	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?	Diterapkan Secara Menyeluruh	3
6.4	II	1	Apakah instansi/perusahaan anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?	Diterapkan Secara Menyeluruh	3
6.5	II	1	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	Diterapkan Secara Menyeluruh	3
6.6	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?	Diterapkan Secara Menyeluruh	3
6.7	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	Diterapkan Secara Menyeluruh	3
6.8	II	1	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	Diterapkan Secara Menyeluruh	3
6.9	II	1	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	Diterapkan Secara Menyeluruh	3
6.10	II	1	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	Diterapkan Secara Menyeluruh	3
6.11	II	1	Apakah instansi/perusahaan anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	Diterapkan Secara Menyeluruh	3
6.12	III	2	Apakah instansi/perusahaan anda mempunyai standar dalam menggunakan enkripsi?	Diterapkan Secara Menyeluruh	6

Gambar 2.8 Tampilan Area Teknologi dan Keamanan Informasi
Sumber: Indeks KAMI 4.2

Total jumlah pertanyaan yang ada di area ini adalah sebanyak 26 pertanyaan dan terbagi menjadi 3 tahap. Jumlah pertanyaan yang terdapat pada pada tahap 1 adalah sebanyak 14 pertanyaan, jumlah pertanyaan yang terdapat pada tahap 2 adalah sebanyak 10 pertanyaan, dan jumlah pertanyaan yang terdapat pada tahap 3 adalah sebanyak 2 pertanyaan. Kategori penilaian pada area ini terdiri dari "Tidak dilakukan", "Dalam Perencanaan", "Dalam Penerapan atau Diterapkan Sebagian", dan "Diterapkan Secara Menyeluruh".

Selain dilakukan evaluasi terhadap lima area tersebut, juga akan dilakukan evaluasi terhadap dua bagian berikut:

- Kategori Sistem Elektronik

  Bagian ini untuk mengevaluasi tingkat atau kategori sistem elektronik yang digunakan. Berikut adalah tampilan pada bagian sistem elektronik:

Bagian I: Kategori Sistem Elektronik			
Bagian ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan			
	[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis	Status	Skor
#	Karakteristik Instansi/Perusahaan		
1.1	Nilai investasi sistem elektronik yang terpasang [A] Lebih dari Rp.30 Miliar [B] Lebih dari Rp.3 Miliar s/d Rp.30 Miliar [C] Kurang dari Rp.3 Miliar	C	1
1.2	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik [A] Lebih dari Rp.10 Miliar [B] Lebih dari Rp.1 Miliar s/d Rp.10 Miliar [C] Kurang dari Rp.1 Miliar	A	5
1.3	Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu [A] Peraturan atau Standar nasional dan internasional [B] Peraturan atau Standar nasional [C] Tidak ada Peraturan khusus	A	5
1.4	Menggunakan teknik kriptografi khusus untuk keamanan informasi dalam Sistem Elektronik [A] Teknik kriptografi khusus yang disertifikasi oleh Negara [B] Teknik kriptografi sesuai standar industri, tersedia secara publik atau dikembangkan sendiri [C] Tidak ada penggunaan teknik kriptografi	B	2
1.5	Jumlah pengguna Sistem Elektronik [A] Lebih dari 5.000 pengguna [B] 1.000 sampai dengan 5.000 pengguna [C] Kurang dari 1.000 pengguna	A	5

Gambar 2.9 Tampilan Bagian Kategori Sistem Elektronik
Sumber: Indeks KAMI 4.2

Total jumlah pertanyaan yang terdapat pada bagian ini adalah 10 pertanyaan. Adapun skor penilaian untuk kategori sistem elektronik adalah sebagai berikut:

- Rendah: apabila skor yang diperoleh sebesar 10-15.
- Tinggi: apabila skor yang diperoleh sebesar 16-34.
- Strategis: apabila skor yang diperoleh sebesar 35-50.

Skor yang telah diperoleh tersebut memiliki korelasi atau hubungan dengan hasil evaluasi akhir atau status kesiapan:

KATEGORI SISTEM ELEKTRONIK				
Rendah		Skor Akhir		Status Kesiapan
10	15	0	174	Tidak Layak
		175	312	Pemenuhan Kerangka Kerja Dasar
		313	535	Cukup Baik
		536	645	Baik
Tinggi		Skor Akhir		Status Kesiapan
16	34	0	272	Tidak Layak
		273	455	Pemenuhan Kerangka Kerja Dasar
		456	583	Cukup Baik
		584	645	Baik
Strategis		Skor Akhir		Status Kesiapan
35	50	0	333	Tidak Layak
		334	535	Pemenuhan Kerangka Kerja Dasar
		536	609	Cukup Baik
		610	645	Baik

Gambar 2.10 Korelasi Antara Kategori Sistem Elektronik dengan Skor Akhir
Sumber: Indeks KAMI 4.2

Gambar 2.10 di atas menunjukkan bahwa hasil evaluasi akhir atau status kesiapan yang terdapat pada *dashboard* ditentukan berdasarkan skor kategori sistem elektronik dan skor akhir atau skor tingkat kelengkapan penerapan ISO 27001.

- Suplemen

Bagian ini untuk mengevaluasi kelengkapan, konsistensi, dan efektivitas penggunaan teknologi dalam pengamanan aset informasi. Berikut adalah tampilan pada bagian suplemen:

Bagian VII: Suplemen

Bagian ini mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
7.1			**Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan**		2.89
7.1.1			**Manajemen Risiko dan Pengelolaan Keamanan pihak ketiga**		
7.1.1.1		1	Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?	Tidak Dilakukan	0
7.1.1.2		1	Apakah instansi/perusahaan mengkomunikasikan dan mengklarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada mereka?	Diterapkan Secara Menyeluruh	3
7.1.1.3		1	Apakah instansi/perusahaan mengklarifikasi persyaratan mitigasi risiko instansi/perusahaan dan ekspektasi mitigasi risiko yang harus dipatuhi oleh pihak ketiga?	Diterapkan Secara Menyeluruh	3
7.1.1.4		1	Apakah rencana mitigasi terhadap risiko yang diidentifikasi tersebut disetujui oleh manajemen pihak ketiga atau karyawan kontrak?	Diterapkan Secara Menyeluruh	3
7.1.1.5		1	Apakah instansi/perusahaan telah menerapkan kebijakan keamanan informasi bagi pihak ketiga secara memadai, mencakup persyaratan pengendalian akses, penghancuran informasi, manajemen risiko penyediaan layanan pihak ketiga, dan NDA bagi karyawan pihak ketiga?	Diterapkan Secara Menyeluruh	3
7.1.1.6		1	Apakah kebijakan tersebut (7.1.1.5) telah dikomunikasikan kepada pihak ketiga dan mereka menyatakan persetujuannya dalam dokumen kontrak, SLA atau dokumen sejenis lainnya?	Diterapkan Secara Menyeluruh	3
7.1.1.7		1	Apakah hak audit TI secara berkala ke pihak ketiga/pihak ketiga telah ditetapkan sebagai bagian dan persyaratan kontrak, dikomunikasikan dan disetujui pihak ketiga? Termasuk di dalamnya akses terhadap laporan audit internal / eksternal tentang kondisi kontrol keamanan informasi pihak ketiga/pihak ketiga?	Diterapkan Secara Menyeluruh	3
7.1.2			**Pengelolaan Sub-Kontraktor/Alih Daya pada Pihak Ketiga**		
7.1.2.1		1	Apakah pihak ketiga sudah mengidentifikasi risiko terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan dalam layanannya?	Diterapkan Secara Menyeluruh	3

Gambar 2.11 Tampilan Bagian Suplemen
Sumber: Indeks KAMI 4.2

Total jumlah pertanyaan yang terdapat pada bagian suplemen adalah 53 pertanyaan. Terdapat 27 pertanyaan untuk bagian pertama, 10 pertanyaan untuk bagian kedua, dan 16 pertanyaan untuk bagian ketiga. Kategori penilaian pada bagian suplemen terdiri dari “Tidak dilakukan”, “Dalam Perencanaan”, “Dalam Penerapan atau Diterapkan Sebagian”, dan “Diterapkan Secara Menyeluruh”.

Jawaban dari setiap pertanyaan pada masing-masing area akan diberi skor sebagai bagian dari evaluasi. Skor ini bertujuan untuk menghasilkan angka indeks dan menampilkan hasil evaluasi pada *dashboard.*

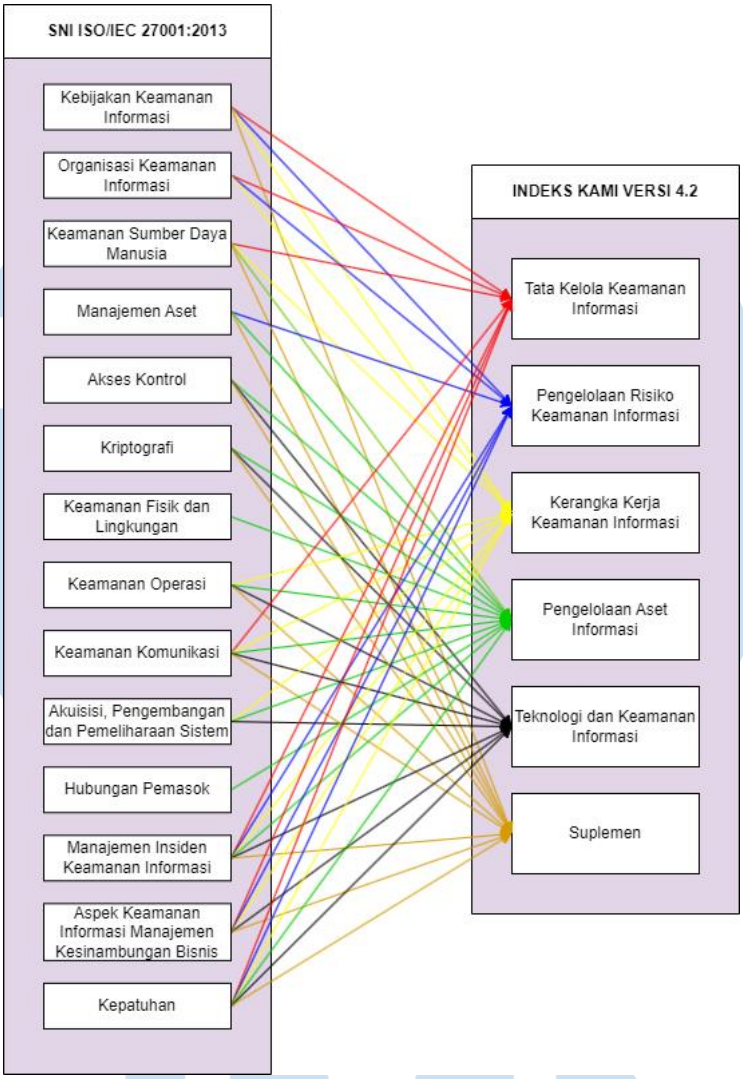
	Kategori Pengamanan		
Status Pengamanan	1	2	3
Tidak Dilakukan	0	0	0
Dalam Perencanaan	1	2	3
Dalam Penerapan atau Diterapkan Sebagian	2	4	6
Diterapkan secara Menyeluruh	3	6	9

Gambar 2.12 Status dan Kategori Pengamanan
Sumber: Indeks KAMI 4.2

Gambar 2.12 di atas menunjukkan bahwa pertanyaan yang ada dalam indeks KAMI (Keamanan Informasi) terbagi menjadi 3 kategori pengamanan, yaitu "1", "2", dan "3". Terdapat juga status pengamanan yang terdiri dari "Tidak Dilakukan", "Dalam Perencanaan", "Dalam Penerapan atau Diterapkan Sebagian", dan "Diterapkan Secara Menyeluruh". Adapun skor yang akan diperoleh dari masing-masing pertanyaan akan ditentukan oleh status pengamanan dan kategori pengamanannya.

2.4 Keterkaitan ISO 27001 dan Indeks KAMI (Keamanan Informasi)

Terdapat korelasi pada masing-masing area pada indeks KAMI (Keamanan Informasi) yang terdiri dari area tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja pengelolaan keamanan informasi, pengelolaan aset informasi, dan teknologi dan keamanan informasi terhadap *Annex A* yang terdapat dalam standar ISO 27001:2013. Korelasi ini menunjukkan bahwa indeks KAMI (Keamanan Informasi) dibuat dengan berdasarkan standar ISO 27001:2013 sehingga dapat membantu mengukur tingkat kematangan dan kepatuhan penerapan ISO 27001:2013. Berikut adalah korelasi ISO 27001:2013 dan indeks KAMI (Keamanan Informasi) 4.2:



Gambar 2.13 Korelasi Indeks KAMI 4.2 dan ISO 27001:2013
Sumber: Hasil Olahan Peneliti

Gambar 2.13 di atas dibuat dengan mengacu kepada penelitian yang dilakukan oleh Ramadhani, et al. [26]. Versi indeks KAMI (Keamanan Informasi) yang digunakan pada penelitian tersebut adalah 4.0, sedangkan pada penelitian ini menggunakan versi 4.2.

2.5 Penelitian Terdahulu

Penelitian ini mengacu kepada 10 penelitian sejenis yang telah ditemukan yang terdiri dari 5 jurnal internasional dan 5 jurnal nasional. Berikut adalah 10 penelitian terdahulu yang menjadi acuan dalam penelitian ini terkait dengan penerapan ISO 27001 dan indeks KAMI (Keamanan Informasi):

Tabel 2.1 Penelitian Terdahulu 1

Judul	Evaluation of the Readiness Level of Information System Security at the BAKAMLA Using the KAMI Index based on ISO 27001:2013
Nama Jurnal	International Journal of Mechanical Engineering
Tahun	2022
Penulis	Peik Sugiarto dan Yohan Suryanto
Masalah	Mengukur dan mengevaluasi tingkat kematangan keamanan informasi serta memberikan rekomendasi perbaikan untuk meningkatkan keamanan informasi di BAKAMLA.
Adopsi	Menggunakan indeks KAMI 4.0 untuk mengukur tingkat kematangan keamanan informasi di BAKAMLA serta memberikan rekomendasi berdasarkan ISO 27001:2013.
Hasil	Sistem elektronik BAKAMLA memperoleh nilai sebesar 17 yang artinya berada dalam kategori "HIGH", sedangkan tingkat kematangan untuk 5 kategori yang diperoleh dari indeks KAMI sebesar 164 atau berada di level I hingga I+, yang artinya belum layak dan perlu adanya perbaikan terhadap 5 kategori, yaitu *governance, asset management, risk management, information security framework,* dan *information technology and security.*

Tabel 2.2 Penelitian Terdahulu 2

Judul	ISO 27001:2013 for Laboratory Management Information System at School of Applied Science Telkom University
Nama Jurnal	IOP Conference Series: Materials Science and Engineering
Tahun	2020
Penulis	Alit Yuniargan Eskaluspita
Masalah	Mengidentifikasi tingkat keamanan informasi pada SIMLAB Universitas Telkom.
Adopsi	Menggunakan ISO 27001:2013 sebagai standar dalam melakukan pengukuran keamanan informasi.
Hasil	Tingkat kematangan keamanan informasi SIMLAB berada di level 2 sehingga perlu adanya perbaikan untuk mencapai standar ISO 27001:2013.

Tabel 2.3 Penelitian Terdahulu 3

Judul	A Comparative Review of ISMS Implementation Based on ISO 27000 Series in Organizations of Different Business Sectors
Nama Jurnal	Journal of Physics: Conference Series
Tahun	2019
Penulis	Zaidatulnajla Hamdi1, Azah Anir Norman, Nurul Nuha Abdul Molok, dan Farkhondeh Hassandoust

Masalah	Membandingkan dan mengetahui sektor bisnis mana yang telah memenuhi standar ISO 27001 terhadap implementasi sistem manajemen keamanan informasi.
Adopsi	Menggunakan ISO 27001 untuk mengukur kepatuhan atau pemenuhan standar ISO 27001 pada masing-masing organisasi.
Hasil	Lembaga Pendidikan memiliki nilai kepatuhan tertinggi terhadap standar ISO 27001, kemudian diikuti oleh *enterprises*, usaha kecil dan menengah, dan lembaga nirlaba. Akan tetapi, semua jenis organisasi tersebut masih belum layak untuk mendapatkan sertifikasi ISO 27001.

Tabel 2.4 Penelitian Terdahulu 4

Judul	Implementation of Security System on Humanitarian Organization: Case Study of Dompet Dhuafa Foundation
Nama Jurnal	Journal of Physics: Conference Series
Tahun	2019
Penulis	Emil R. Kaburuan dan ASL Lindawati
Masalah	Dompet Dhuafa Foundation mengalami ancaman keamanan terkait dengan transaksi dan pengolahan data serta informasi donator. Selain itu, Dompet Dhuafa Foundation juga ingin mengetahui kondisi sistem keamanan dari DESI (Dompet Dhuafa Information System).
Adopsi	Mengimplementasikan otentikasi ke semua akun, menerapkan enkripsi, menggunakan antivirus, menggunakan *firewall*, membuat segregasi tugas, menerapkan SOP, serta menggunakan ISO 27001 sebagai standar keamanan informasi.
Hasil	Dengan menerapkan standar ISO 27001:2013, Dompet Dhuafa Foundation mampu melindungi kerahasiaan, integritas, dan ketersediaan informasi serta mampu mengendalikan risiko-risiko yang muncul terkait dengan keamanan informasi.

Tabel 2.5 Penelitian Terdahulu 5

Judul	Information Safety Process Development According to ISO 27001 for an Industrial Enterprise
Nama Jurnal	Procedia Manufacturing
Tahun	2019
Penulis	Nelli V. Syreyshchikovaa, Danil Yu. Pimenova, Tadeusz Mikolajczyk, dan Liviu Moldovan
Masalah	Adanya pelanggaran keamanan informasi yang terdiri dari pengungkapan informasi kepada pihak ketiga, akses informasi yang tidak sah, kualifikasi untuk spesialis perlindungan informasi rendah, rendahnya implementasi terhadap pembuatan sistem keamanan informasi, kurangnya

	pemahaman karyawan terkait dengan pentingnya melindungi informasi, dan masalah-masalah yang bersifat politik.
Adopsi	Merancang, mengembangkan, dan menguasai proses keamanan informasi sesuai dengan ISO 27001.
Hasil	Tercapainya perancangan, pengembangan, dan penguasaan proses keamanan informasi yang sesuai dengan ISO 27001 serta masalah-masalah yang terjadi tersebut berhasil diatasi.

Tabel 2.6 Penelitian Terdahulu 6

Judul	Evaluasi Tata Kelola Keamanan Teknologi Informasi Menggunakan Indeks KAMI Untuk Persiapan Standar SNI ISO/IEC 27001 (Studi Kasus: STMIK Mardira Indonesia)
Nama Jurnal	Jurnal Computech & Bisnis
Tahun	2020
Penulis	Asep Ririh Riswaya, Ashwin Sasongko, dan Asep Maulana
Masalah	Mengetahui tingkat keamanan teknologi informasi di PUSKOMTEK
Adopsi	Menggunakan indeks KAMI 4.0 untuk mengetahui tingkat keamanan teknologi informasi di PUSKOMTEK STMIK-MI sesuai dengan standar SNI ISO/IEC 27001.
Hasil	Sektor elektronik memperoleh nilai sebesar 21 yang artinya tinggi, sedangkan untuk tingkat kesiapan dan kematangan keamanan teknologi informasi berada di level I kebawah, yang artinya belum layak SNI ISO/IEC 27001.

Tabel 2.7 Penelitian Terdahulu 7

Judul	SNI ISO/IEC 27001 dan Indeks KAMI: Manajemen Risiko PUSDATIN (PUPR)
Nama Jurnal	Ultima Infosys : Jurnal Ilmu Sistem Informasi
Tahun	2021
Penulis	Piski Sundari dan Wella
Masalah	Mengetahui tingkat kesiapan dan kematangan keamanan informasi PUSDATIN.
Adopsi	Menggunakan indeks KAMI untuk mengetahui kesiapan dan kematangan PUSDATIN dalam menuju sertifikasi ISO 27001:13
Hasil	Tingkat kepentingan TIK sebesar 39, artinya berada dalam kategori “KRITIS”. Selain itu, level kematangan PUSDATIN adalah level I+, artinya perlu dilakukan perbaikan terhadap keamanan informasi.

Tabel 2.8 Penelitian Terdahulu 8

Judul	Evaluasi Tingkat Kesiapan Keamanan Informasi Pada Lembaga Pendidikan Menggunakan Indeks Kami 4.0
Nama Jurnal	Jurnal Mobile and Forensics (MF)
Tahun	2019

Penulis	Pramudhita Ferdiansyah, Subektiningsih, dan Rini Indrayani
Masalah	Terdapat banyak data informasi pada UPTD XYZ sehingga diperlukan evaluasi keamanan informasi guna mengukur tingkat kesiapan, kematangan, dan kelengkapan keamanan informasi yang ada.
Adopsi	Menggunakan indeks KAMI 4.0 untuk melakukan evaluasi kematangan dan tata kelola keamanan informasi sesuai dengan standar ISO/IEC 27001:2017.
Hasil	Untuk kebutuhan sistem elektronik, hasil yang diperoleh adalah sebesar 20, sedangkan hasil yang diperoleh untuk tingkat kelengkapan informasi adalah sebesar 245. Hasil tersebut menunjukkan bahwa tingkat keamanan informasi masih sangat rendah dan belum layak melakukan sertifikasi ISO/IEC 27001 sehingga perlu adanya perbaikan.

Tabel 2.9 Penelitian Terdahulu 9

Judul	Penilaian Keamanan Informasi E-Government Menggunakan Index Keamanan Informasi (KAMI) 4.0
Nama Jurnal	Jurnal Teknologi Informasi dan Komputer
Tahun	2020
Penulis	I Gede Putu Krisna Juliharta, Komang Tri Werthi, dan Ni Luh Putu Ning Septyarini Putri Astawa
Masalah	Memperkuat sistem manajemen pengamanan informasi di Pemerintah Kota Denpasar dalam pelaksanaan *e-government.*
Adopsi	Menggunakan indeks keamanan informasi (KAMI) 4.0 untuk melakukan proses pengukuran.
Hasil	Hasil akhir yang diperoleh dari indeks KAMI, yaitu total skor kematangan pada Pemerintah Kota Denpasar adalah 74 sehingga tingkat kematangannya berada di level I-I+. Berdasarkan hasil tersebut, maka Pemerintah Kota Denpasar termasuk kategori kondisi awal atau reaktif. Untuk mendapatkan sertifikasi ISO 27001:2013, maka Pemerintah Kota Denpasar perlu melakukan perbaikan untuk meningkatkan level sistem manajemen keamanan informasinya.

Tabel 2.10 Penelitian Terdahulu 10

Judul	Evaluasi Manajemen Keamanan Informasi Pada Perusahaan Pemula Berbasis Teknologi Menggunakan Indeks KAMI
Nama Jurnal	Jurnal SimanteC
Tahun	2022
Penulis	Aprilian Lisa Maryanto, Moh Noor Al Azam, dan Aryo Nugroho
Masalah	Perusahaan pernah mengalami insiden kehilangan data dan belum pernah melakukan evaluasi terhadap keamanan informasi. Oleh karena itu, dilakukan evaluasi terhadap

	keamanan informasi untuk mengetahui tingkat kesiapan penerapan keamanan informasi.
Adopsi	Menggunakan indeks KAMI 4.0 untuk melakukan pengukuran terhadap tingkat kematangan dan kelengkapan manajemen informasi berdasarkan ISO 27001:2013.
Hasil	Tingkat kematangan dan kelengkapan manajemen informasi perusahaan tersebut berada di level I hingga I+, yang artinya belum layak dan perlu adanya rekomendasi untuk perbaikan.

Berdasarkan penelitian sebelumnya yang terdapat di atas, terdapat kesamaan antara penelitian terdahulu dengan penelitian yang sedang dilakukan, yaitu menggunakan *tools* indeks KAMI (Keamanan Informasi) untuk mengukur tingkat kematangan keamanan informasi dan kepatuhan penerapan standar ISO 27001 pada suatu perusahaan dalam rangka meningkatkan dan memperkuat keamanan informasi perusahaan [6]-[11]. Selain memanfaatkan alat bantu *tools* indeks KAMI (Keamanan Informasi), pengukuran tingkat kematangan keamanan informasi dan kepatuhan penerapan standar ISO 27001 juga dapat dilakukan dengan hanya menggunakan ISO 27001 [5]. Standar ISO 27001 juga digunakan oleh berbagai sektor bisnis, baik lembaga pendidikan, *enterprises*, usaha kecil dan menengah ataupun lembaga nirlaba untuk mengukur tingkat kematangan sistem informasi [12]. Standar ISO 27001 ini dapat digunakan oleh perusahaan untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi serta mengendalikan risiko ancaman keamanan informasi yang muncul [13]. Selain mengendalikan risiko yang muncul, ISO 27001 juga dapat mengatasi pelanggaran keamanan informasi yang terjadi pada perusahaan [14].

Selain adopsi, terdapat juga perbedaan atau kebaruan dari penelitian ini, yaitu objek penelitian dan versi indeks KAMI (Keamanan Informasi) yang digunakan. Pada penelitian sebelumnya masih jarang ditemukan adanya perusahaan swasta yang dijadikan objek penelitian serta belum ditemukan adanya penelitian terkait dengan evaluasi sistem manajemen keamanan informasi terhadap perusahaan yang bergerak dibidang kontraktor dan *developer*. Selain itu, penelitian sebelumnya menggunakan versi indeks KAMI (Keamanan Informasi) 4.0,

sedangkan penelitian ini menggunakan versi indeks KAMI (Keamanan Informasi) 4.2.