KOMINFO

DIGITAL TALENT SCHOLARSHIP

GTA Government Transformation Academy

MODUL PELATIHAN

PEMAHAMAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERBASIS SNI ISO/IEC 27001:2013

DAFTAR ISI

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 DEFINISI

The International Organization for Standardization (ISO) merupakan sebuah organisasi internasional yang mengembangkan dan menerbitkan standar internasional. Beranggotakan badan-badan standardisasi nasional, beberapa diantaranya BSN (Badan Standardisasi Nasional - Indonesia), BSI (British Standard Institution - Inggris), ANSI (American National Standard Institute - Amerika) dan lain-lain. ISO sendiri bukan merupakan singkatan dari apapun melainkan berasal dari bahasa yunani isos yang berarti setara atau serupa.

Sistem Manajemen Keamanan Informasi (SMKI) adalah pendekatan sistematis untuk mengelola informasi perusahaan yang sensitif sehingga tetap aman. Ini termasuk orang, proses dan sistem TI (Teknologi Informasi) dengan menerapkan proses manajemen resiko. Ini dapat membantu bisnis kecil, menengah dan besar di sektor apa pun. Sistem Manajemen Keamanan Informasi terdiri dari kebijakan, prosedur, pedoman, dan sumber daya serta aktivitas terkait, yang dikelola secara kolektif oleh suatu organisasi, dalam upaya melindungi aset informasinya.

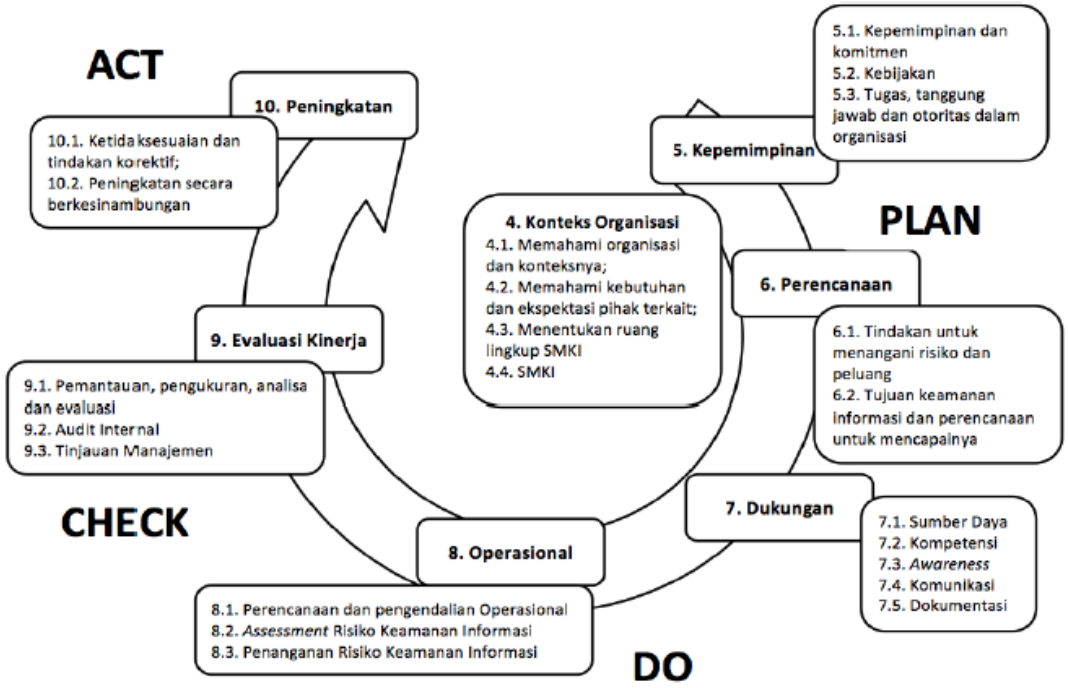
ISO/IEC 27001:2013 adalah kerangka kerja manajemen untuk perlindungan informasi penting bisnis. Bukan standar teknis yang menjelaskan SMKI secara detail teknis. Itu tidak fokus pada Teknologi Informasi saja, tetapi juga yang lain aset bisnis penting, sumber daya, dan proses dalam organisasi. Versi ini adalah versi terbaru dari versi sebelumnya ISO/IEC 27001:2005. SNI ISO/IEC 27001:2013 adalah standar adopsi dari ISO/IEC 27001:2013 yang dikeluarkan oleh BSN. SNI ISO/IEC 27001:2013 terdiri dari 2 (dua) bahasa yaitu Bahasa Inggris dan Bahasa Indonesia.

Struktur SNI ISO/IEC 27001:2013 terdiri dari 10 klausul dan lampiran Anex. Klausul 4 -10 tidak dapat dikecualikan dalam sertifikasi SNI ISO/IEC 27001:2013. Kebutuhan utama SNI ISO/IEC 27001:2013 dibentuk dalam sebuah siklus SMKI. Siklus tersebut terdiri dari *Plan – Do – Check – Act* (PDCA *Cycle*).

Total klausul wajib pada SNI ISO/IEC 27011:2013 ada 7 (tujuh), yaitu :

- Klausul 4 : Konteks Organisasi
- Klausul 5 : Kepemimpinan
- Klausul 6 : Perencanaan
- Klausul 7 : Dukungan
- Klausul 8 : Operasional
- Klausul 9 : Evaluasi Kinerja
- Klausul 10 : Peningkatan

Siklus PDCA apabila digambarkan terkait dengan klausul dari SNI ISO/IEC 27001:2013 adalah sebagai berikut :



GAMBAR 1. SIKLUS PDCA TERKAIT KLAUSUL SNI ISO/IEC 27001:2013

Lampiran Anex atau control area pada SNI ISO/IEC 27001:2013 terbagi menjadi beberapa bagian sebagai berikut :

- A.5 - A.18: 14 domain kontrol.
- 35 mengontrol tujuan.
- 114 kontrol.

SNI ISO/IEC 27001:2013 Control Point and Control Objective		
Annex	**Deskripsi**	**total Kontrol**
A5	Kebijakan Keamanan Informasi	**2**
A6	Organisasi Keamanan informasi	**7**
A7	Keamanan Sumber Daya Manusia	**6**
A8	Manajemen Aset	**10**
A9	Kendali Akses	**14**
A10	Kriptografi	**2**
A11	Keamanan Fisik dan Lingkungan	**15**
A12	Keamanan Operasi	**14**
A13	Keamanan Komunukasi	**7**
A14	Akuisisi, Pengembangan dan Perawatan Sistem	**13**
A15	Hubungan Pemasok	**5**
A16	Manajemen Insiden Keamanan Informasi	**7**
A17	Aspek Keamanan Informasi dari Manajemen Keberlangsungan	**4**
A18	Kesesuaian	**8**
Total Kontrol		**114**

GAMBAR 2. LAMPIRAN ANEX PADA SNI ISO/IEC 27001:2013

1.2 LATAR BELAKANG

Hal-hal yang erat kaitannya dalam terbentuknya SNI ISO/IEC 27001:2013 diantaranya ialah potensi pelanggaran informasi dapat merusak reputasi organisasi, ketersediaan informasi sangat penting setiap saat, kurangnya kepercayaan pada kemampuan organisasi untuk mengelola resiko keamanan informasi, kesulitan dalam menanggapi ekspektasi pelanggan yang meningkat sehubungan dengan keamanan informasi mereka, tidak ada kesadaran akan keamanan informasi di dalam organisasi, dan adanya peningkatan denda untuk pelanggaran data pribadi (salah satu aset organisasi) membuat organisasi perlu memastikan kepatuhan dengan persyaratan legislative, seperti Undang-Undang Perlindungan Data Indonesia.

1.3 TUJUAN

Adapun tujuan SNI ISO/IEC 27001:2013 yaitu berhubungan dengan pendekatan menyeluruh dalam melindungi dan mempertahankan keamanan informasi yang terdiri dari 3 (tiga) aspek yaitu *Confidentiality* (Kerahasiaan), *Integrity* (Integritas) dan *Availability* (Ketersediaan). Pengertian dari ketiga aspek tersebut dijabarkan sebagai berikut :

a. *Confidentiality* (Kerahasiaan) yaitu memastikan informasi hanya dapat diakses oleh pihak yang berkepentingan atau dapat juga dijelaskan sebagai informasi bersifat rahasia dan harus dilindungi terhadap keterbukaan dari pengguna yang tidak berkepentingan.
b. *Integrity* (Integritas) yaitu menjamin keakuratan dan kelengkapan informasi dan pengolahan informasi diantaranya layanan, fungsi sistem, dan informasi harus terjamin dan tersedia bagi pengguna saat diperlukan.
c. *Availability* (Ketersediaan) yaitu menjamin bahwa pengguna yang berwenang dapat mengakses informasi saat dibutuhkan termasuk informasi harus komplit dan tidak dirubah. Dalam teknologi informasi, kata informasi terkait dengan berita. Hilangnya integritas informasi berarti berita tersebut tidak akurat.

GAMBAR 3. TUJUAN SNI ISO/IEC 27001:2013

BAB II

ORGANISASI

2.1 MEMAHAMI ORGANISASI DAN KONTEKSNYA

Organiasi adalah bagian dari klausul 4 SMKI SNI ISO/IEC 27001:2013. Pada siklus PDCA, klasul ini masuk ke dalam siklus ‘Plan’. Tujuan dari klausul ini adalah memahami konteks organisasi atau permasalahan organisasi yaitu isu internal dan eksternal yang berkait dengan tujuan suatu organsasi. Informasi mengenai konteks organisasi atau isu internal dan eksternal dapat diperoleh dari berbagai sumber. Sumber antara lain dari:

a. Kajian dokumen-dokumen yang berlaku di perusahaan seperti hasil internal meeting, hasil audit internal, rapat tinjauan manajemen, rencana strategis (renstra), dan dokumen-dokumen penting lainya yang membantu dalam penetapan permasalahan internal.
b. Kajian SWOT Analisa atau analisa *Strengths, Weaknesses, Opportunities* dan *Threats analysis*.
c. Metode *brainstorming* dengan bantuan kalimat tanya "*What if*"
d. Informasi yang diperoleh hasil *meeting* dengan pelanggan atau *supplier*
e. Informasi dari asosiasi profesional
f. Sumber-sumber relevan lainnya

2.2 MEMAHAMI KEBUTUHAN DAN HARAPAN DARI PIHAK YANG BERKEPENTINGAN

Maksud dan tujuan dari klausul ini yaitu untuk menegaskan bahwa bukan hanya persyaratan pelanggan saja yang harus dipenuhi dalam menjalankan roda organisasi, namun terdapat beberapa persyaratan pihak-pihak berkepentingan lain yang perlu dipertimbangkan.

Pihak-pihak yang berkepentingan itu (*stakeholders*) unik untuk setiap organisasi. Setiap organisasi memiliki stakeholders yang berbeda-beda.

Karenanya setiap organisasi harus menentukan pihak-pihak yang berkepentingan sesuai dengan bidang organisasi.

2.3 PENENTUAN RUANG LINGKUP SMKI

Menentukan ruang lingkup SMKI adalah salah satu tonggak utama dalam implementasi. Lingkupnya harus diperiksa dan ditetapkan dengan mempertimbangkan masalah internal dan eksternal, pihak yang berkepentingan dan kebutuhan mereka dan harapan, serta kewajiban kepatuhan terhadap hukum dan peraturan. Pertimbangan tambahan yang diperlukan untuk ruang lingkup SMKI adalah produk, layanan, dan ukuran organisasi, sifat dan kompleksitas. Ruang lingkup dan pengecualiannya harus disimpan sebagai informasi yang terdokumentasi.

2.4 SISTEM MANAJEMEN KEAMANAN INFORMASI

Klausul ini adalah untuk menetapkan, menerapkan, memelihara dan terus meningkatkan SMKI sesuai dengan persyaratan standar.

BAB III

KEPEMIMPINAN

3.1 KEPEMIMPINAN DAN KOMITMEN

Kepemimpinan adalah bagian dari klausul 5 SMKI SNI ISO/IEC 27001:2013. Pada siklus PDCA, klasul ini masuk ke dalam siklus ‘Plan’. Klausul ini mensyaratkan Top Manajemen menunjukkan komitmennya terhadap SMKI dengan memastikan terjadinya integrasi prasyarat SMKI ke dalam proses organisasi. Ini ditunjukkan dengan dinyatakannya pelaksana pengelolaan resiko keamanan informasi berada pada unit terkait. Ditunjuknya unit terkait diperjelas dalam Keputusan Top Manajemen mengenai fungsi dan tugas unit tersebut.

3.2 KEBIJAKAN

Top Manajemen harus menetapkan kebijakan keamanan informasi dengan ketentuan :

a. sesuai dengan tujuan organisasi
b. termasuk tujuan keamanan informasi atau menyediakan kerangka kerja untuk menetapkan tujuan keamanan informasi
c. termasuk komitmen untuk memenuhi persyaratan yang berlaku terkait keamanan informasi
d. termasuk komitmen untuk perbaikan berkelanjutan dari sistem manajemen keamanan informasi.

Sedangkan syarat kebijakan keamanan informasi yaitu harus tersedia sebagai informasi yang terdokumentasi, dikomunikasikan dalam organisasi dan tersedia untuk pihak yang berkepentingan, sebagaimana diperlukan.

3.3 PERAN ORGANISASI, TANGGUNG JAWAB, DAN WEWENANG

Tanggung jawab dan wewenang harus didefinisikan dengan tepat dan dikomunikasikan ke semua tingkatan hierarki dalam organisasi.

BAB IV

PERENCANAAN

4.1 TINDAKAN UNTUK MENANGANI RESIKO DAN PELUANG

Perencanaan adalah bagian dari klausul 6 SMKI SNI ISO/IEC 27001:2013. Pada siklus PDCA, klasul ini masuk ke dalam siklus ‘Plan’. Dalam merencanakan Sistem Manajemen Keamanan Informasi (SMKI), organisasi harus menentukan resiko dan opportunity, agar ketiga kriteria di bawah ini terpenuhi :

a. menjamin tujuan SMKI tercapai
b. mencegah atau mengurangi dampak yang merugikan
c. memastikan continual improvement selalu dilakukan

Untuk memenuhi ketiga kriteria di atas, rencana organisasi harus meliputi :

a. mendefinisikan aksi-aksi yang perlu dilakukan untuk mengatasi resiko dan *opportunity*
b. menentukan cara untuk mengintegrasikan aksi-aksi pada poin a ke dalam proses SMKI serta mengevaluasi tingkat efektivitas dari aksi-aksi tersebut.

4.1.1 Risk assessment keamanan informasi

Proses risk assessment keamanan informasi harus meliputi hal-hal berikut :

a. membuat dan selalu memperbaiki risk criteria keamanan informasi, termasuk *risk acceptance criteria* dan kriteria untuk melakukan proses risk assessment keamanan informasi.
b. proses risk assessment keamanan informasi yang dilakukan secara berkala harus menghasilkan data yang konsisten, valid, dan dapat dikomparasi.

c. mengidentifikasi resiko-resiko keamanan informasi yang terdiri dari proses *risk assessment* keamanan informasi harus mengidentifikasi resiko-resiko yang terkait dengan kerahasiaan, integritas, dan keteradaan informasi yang mana informasi tersebut masih dalam lingkup SMKI dan terakhir menentukan *risk owner*.
d. menganalisa resiko-resiko keamanan informasi yang terdiri dari mendefinisikan konsekuensi-konsekuensi yang dapat terjadi jika resiko-resiko yang telah diidentifikasi pada poin c akan terwujud, menentukan probabilitas terjadinya resiko-resiko yang telah diidenfikasi pada poin c dan menentukan level resiko.
e. mengevaluasi resiko-resiko keamanan informasi yang terdiri dari membandingkan hasil risk analysis dengan risk criteria yang telah ditentukan pada poin a dan membuat prioritas untuk masing-masing hasil *risk analysis*.

4.1.2 Risk treatment keamanan informasi

Proses *risk treatment* keamanan informasi harus meliputi hal-hal berikut :

a. berdasarkan hasil risk assessment, pilih salah satu opsi *risk treatment* keamanan informasi yang tepat
b. menentukan seluruh kontrol yang diperlukan untuk mendukung pengimplementasian *risk treatment* keamanan informasi yang telah dipilih pada poin a
c. bandingkan seluruh kontrol yang telah ditentukan pada poin b dengan seluruh kontrol yang telah diberikan pada Annex A melalui *Statement Of Applicability* (SOA) sehingga diketahui dua hal berikut :

    - alasan dipilih atau tidak dipilihnya kontrol Annex A dan
    - untuk kontrol Annex A yang dipilih, berikan deskripsi singkat tentang cara pengimplementasian kontrol (jika kontrol tersebut baru akan diimplementasi) atau tingkat efektivitas pengimplementasian kontrol (jika kontrol tersebut sudah dan masih diimplementasi)

d. berdasarkan kontrol-kontrol yang telah dipilih, buat perencanaan untuk mengimplementasi *risk treatment* keamanan informasi
e. rencana pengimplementasian *risk treatment* yang telah dibuat beserta *residual risk*-nya harus disetujui oleh *risk owner*.

4.2 SASARAN KEAMANAN INFORMASI DAN PERENCANAAN UNTUK MENCAPAINYA

Sasaran keamanan dan pendokumentasiannya meliputi monitoring implementasi manajemen resiko, pelaporan berkala (*risk reporting*), menjaga pengembangan kompetensi yang berkelanjutan dan melakukan *review* melalui *Risk Management Index*, Survei Budaya Resiko maupun penilaian Tingkat Maturitas Implementasi

Evaluasi atas efektivitas Sistem Manajemen Resiko dilakukan secara berkala meliputi aktivitas:

a. *Review dan monitoring* implementasi manajemen resiko unit secara berkala setiap tiga bulan
b. Penyusunan Laporan Analisa Resiko dan Kepatuhan secara berkala setiap tiga bulan
c. Rapat pembahasan terkait resiko di tingkat Top Manajemen
d. Melakukan pengukuran implementasi budaya resiko melalui survey kepada sejumlah responden
e. Melakukan pengukuran tingkat kematangan implementasi manajemen resiko (ERM *Maturity Level*)

BAB V

DUKUNGAN

5.1 SUMBER DAYA

Perencanaan adalah bagian dari klausul 7 SMKI SNI ISO/IEC 27001:2013. Pada siklus PDCA, klasul ini masuk ke dalam siklus ‘Plan’. Organisasi harus menentukan dan menyediakan sumber daya yang dibutuhkan untuk pembangunan, implementasi, pemeliharaan dan peningkatan berkelanjutan dari sistem manajemen keamanan informasi.

5.2 KOMPETENSI

Klausul ini mensyaratkan bahwa organisasi diantaranya harus menentukan kompetensi orang yang melakukan pekerjaan pada SMKI, menentukan orang yang dianggap kompeten berdasarkan pendidikan, pelatihan atau pengalaman yang relevan. Jika diperlukan, memberi pelatihan untuk memperoleh kompetensi yang diperlukan dan mengevaluasi efektivitas pelatihan tersebut, terakhir harus menyimpan bukti di atas untuk keperluan audit.

5.3 KEPEDULIAN

Klausul ini mensyaratkan bahwa orang yang melakukan pekerjaan dibawah kendali organisasi harus menyadari kebijakan keamanan informasi. Pihak ketiga dan personilnya yang mendapatkan akses terhadap organisasi organisasi harus menandatangani *Confidentiality Agreement* (NDA : *Non Disclosure Agreement* dan Personel NDA) sebelum yang bersangkutan melaksanakan pekerjaan untuk kepentingan organisasi.

5.4 KOMUNIKASI

Organisasi harus menentukan komunikasi internal dan eksternal yang relevan dengan Sistem Manajemen Keamanan Informasi termasuk dalam hal apa harus berkomunikasi, kapan diperlukan komunikasi, dengan siapa komunikasi dilakukan, siapa yang harus berkomunikasi, dan proses dimana komunikasi akan dilakukan.

5.5 INFORMASI TERDOKUMENTASI

Klausul ini mensyaratkan organisasi untuk mendokumentasikan informasi yang diperlukan organisasi untuk memastikan efektivitas Sistem Manajemen Keamanan Informasi.

BAB VI

OPERASIONAL

6.1 PERENCANAAN DAN PENGENDALIAN OPERASIONAL

Operasional adalah bagian dari klausul 8 SMKI SNI ISO/IEC 27001:2013. Pada siklus PDCA, klasul ini masuk ke dalam siklus ‘Do’. Pada klausul ini hal selanjutnya yang dilakukan organisasi adalah organisasi harus merencanakan, menerapkan dan mengendalikan proses yang diperlukan untuk memenuhi persyaratan kemanan informasi. Dalam hal perencanaan, penerapan dan pengendalian organisasi harus mengacu kepada perencanaan resiko yang telah tertuang dalam klausul 6. Selain itu pada saat menerapkan rencana, capaian yang ditetapkan harus sesuai dengan sasaran resiko yang telah dibuat sesuai klausul 6. Identifikasi resiko dilakukan untuk mengidentifikasi semua resiko yang dihadapi oleh organisasi di dalam ruang lingkup SMKI. Beberapa contoh identifikasi resiko terdiri dari identifikasi aset, ancaman, kontrol keamanan yang ada, dan kerentanan yang saling terkait.

Informasi pada proses perencanaan, penerapan dan pengendalian harus disimpan dan didokumentasikan yang diperlukan untuk memastikan bahwa proses telah dilakukan sesuai yang direncanakan. Selanjutnya organisasi harus mengendalikan perubahan yang terjadi pada hal-hal yang sudah direncanakan dan harus mengevaluasi konsekuensi dari perubahan tersebut termasuk perubahan yang tidak diinginkan, sehingga dapay mengambil tindakan seperlunya untuk mengurangi resiko atau efek buruk. Klausul ini juga memerintahkan bahwa organisasi harus memastikan bahwa proses yang dialih dayakan telah ditetapkan dan dikendalikan.

6.2 PENILAIAN RESIKO KEAMANAN INFORMASI

Apabila perencanaan dan pengendalian telah dilakukan maka selanjutnya organisasi harus melakukan penilaian resiko keamanan informasi pada selang waktu yang telah direncanakan atau ketika perubahan signifikan diusulkan atau terjadi, dengan mempertimbangkan criteria resiko yang telah

dibuat. Hasil penilaian resiko keamanan informasi harus disimpan dan didokumentasikan.

6.3 PENANGANAN RESIKO KEAMANAN INFORMASI

Organisasi harus menerapkan rencana penanganan resiko keamanan informasi yang telah dibuat pada klausul 6, contoh : penanganan insiden dari resiko keamanan informasi. Proses penanganan resiko kemanan informasi harus disimpan dan didokumentasikan.

BAB VII

EVALUASI KINERJA

7.1 PEMANTAUAN, PENGUKURAN, ANALISIS DAN EVALUASI

Evaluasi kinerja adalah bagian dari klausul 9 SMKI SNI ISO 27001:2013. Pada siklus PDCA, klausul ini masuk ke dalam siklus ‘Check’. Pada tahap ini organisasi harus mengevaluasi kinerja keamanan informasi dan efektifitas SMKI. Hal yang perlu ditentukan diantaranya :

a. Apa yang perlu dipantau dan diukur, termasuk proses dan pengendalian keamanan informasi
b. Siapa yang harus memantau dan mengukur
c. Kapan pemantauan dan pengukuran dilakukan
d. Siapa yang harus menganalisis dan mengevaluasi hasil
b. Kapan hasil dari pemantauan dan pengukuran dianalisis dan dievaluasi
c. Tetapkan metode untuk pemantauan, pengukuran, analisis dan evaluasi. Pastikan penerapan metode dapat menghasilkan hasil yang valid. Sesuai acuan standar klausul 9.1 yang dimaksud hasil yang valid berupa hasil yang dapat dibandingkan dan dapat diproduksi ulang untuk dinyatakan valid.

Contoh dokumen yang ada pada klausul ini adalah dokumen sasaran mutu. Semua proses dan hasil pemantauan harus disimpan dan didokumentasikan.

7.2 AUDIT INTERNAL

Audit internal menjadi syarat wajib pada klausul 9 SNI ISO 27001:2013. Adanya audit internal diharapkan mampu memantau dan mengukur SMKI serta dapat mempromosikan peningkatan berkelanjutan dari SMKI. Sesuai dengan klausul 9 maka organisasi harus melakukan audit internal pada waktu yang direncanakan dan membahas apakah SMKI sudah sesuai dengan persyaratan yang ditetapkan organisasi untuk SMKI dan apakah SMKI sudah sesuai dengan SNI ISO 27001:2013 secara keseluruhan. Audit internal juga menilai apakah SMI diimplementasikan dan dipelihara secara efektif.

Syarat yang harus dipenuhi dari program audit internal ini sesuai dengan klausul 9 ialah sebagai berikut :

a. Organisasi harus merencanakan, menetapkan, menerapkan dan memelihara program audit, termasuk diantaranya frekuensi, metode, tanggung jawab, persyaratan perencanaan dan pelaporan. Program audit harus mempertimbangkan pentingnya proses yang bersangkutan dan hasil audit sebelumnya.
b. Organisasi harus menentukan kriteria dan ruang lingkup audit
c. Organisasi harus memilih auditor dan menjamin objektivitas dan ketidakberpihakan proses audit
b. Organiasi harus memastikan bahwa hasil audit dilaporkan kepada manajemen terkait SMKI
c. Organiasi harus menyimpan dan mendokumentasikan proses dan hasil audit internal sebagai alat bukti dari program audit

7.3 REVIU MANAJEMEN

Pada klausul ini manajemen puncak dituntut untuk harus mereviu organisasi SMKI pada waktu yang direncanakan. Reviu bertujuan untuk memastikan kesesuaian, kecukupan dan efektifitas. Hal-hal yang mencakup reviu manajeman adalah sebagai berikut :

a. Status tindakan dari reviu manajemen sebelumnya
b. Perubahan isu eksternal dan internal terkait SMKI
b. Umpan balik dari kinerja keamanan informasi, termasuk ketidaksesuaian dan tindakan korektif, hasil pemantauan dan pengukuran, hasil audit dan pemenuhan sasaran keamanan informasi
c. Umpan balik dari pihak yang berkepentingan
d. Hasil dari penilaian resiko dan status rencana penanganan resiko
e. Peluang untuk perbaikan berkelanjutan

Organiasi harus menyimpan dan mendokumentasikan proses manajemen reviu sebagai alat bukti hasil reviu manajemen.

BAB VIII

PERBAIKAN

8.1 KETIDAKSESUAIAN DAN TINDAKAN KOREKTIF

Perbaikan adalah bagian dari klausul 10 SMKI SNI ISO/IEC 27001:2013. Klausul ini adalah klausul akhir. Pada siklus PDCA, klausul ini masuk ke dalam siklus ‘Act’. Ketidaksesuaian yang dimaksud dalam SMKI ialah tidak terpenuhinya persyaratan SMKI sesuai SNI ISO 27001:2013. Klausul 10 mengatur jika ditemukan adanya ketidaksesuaian, maka organisasi harus :

a. Mengambil tindakan terhadap ketidaksesuaian agar dapat mengendalikan dan mengoreksinya serta mampu menangani konsekuensinya.
b. Melakukan evaluasi tindakan untuk menghilangkan penyebab ketidaksesuaian, dengan tujuan hal tersebut tidak terulang atau terjadi lagi. Tindakan tersebut diantaranya mereviu ketidaksesuaian, menentukan penyebab ketidaksesuaian, dan menentukan apakah ada ketidaksesuaian serupa atau berpotensi terjadi kembali.
c. Melaksanakan tindakan apapun yang diperlukan.
d. Mereviu efektifitas tindakan korektif yang diambil.
e. Membuat perubahan pada SMKI jika diperlukan. Perubahan yang dilakukan harus sesuai dengan efek dari ketidaksesuaian yang ditemukan.
f. Menyimpan dan mendokumentasikan semua sifat ketidak sesuaian beserta tindakan yang diambil termasuk hasil dari tindakan korektif.

8.2 PERBAIKAN BERKELANJUTAN

Tahap akhir pada klausul 10 ini menyebut bahwa organisasi harus terus memperbaiki kesesuaian, kecukupan dan efektifitas SMKI.

BAB IX

TAHAPAN PROSES PENERAPAN SNI ISO/IEC 27001:2013

9.1 KOMITMEN MANAJEMEN

Manajemen puncak adalah orang atau kelompok orang yang mengarahkan dan mengendalikan suatu organisasi pada tingkat tertinggi dimana yang menjabat sebagai manajemen puncak bergantung pada jenis organisasi. Contohnya, manajemen puncak pada perusahaan adalah dewan direksi, sedangkan manajemen puncak pada kementerian adalah menteri. Jika lingkup penerapan sistem manajemen hanya mencakup sebagian organisasi, manajemen puncak adalah orang yang mengarahkan dan mengendalikan bagian organisasi itu. Misalnya, kepala departemen pada suatu perusahaan atau direktur jenderal pada suatu kementerian.

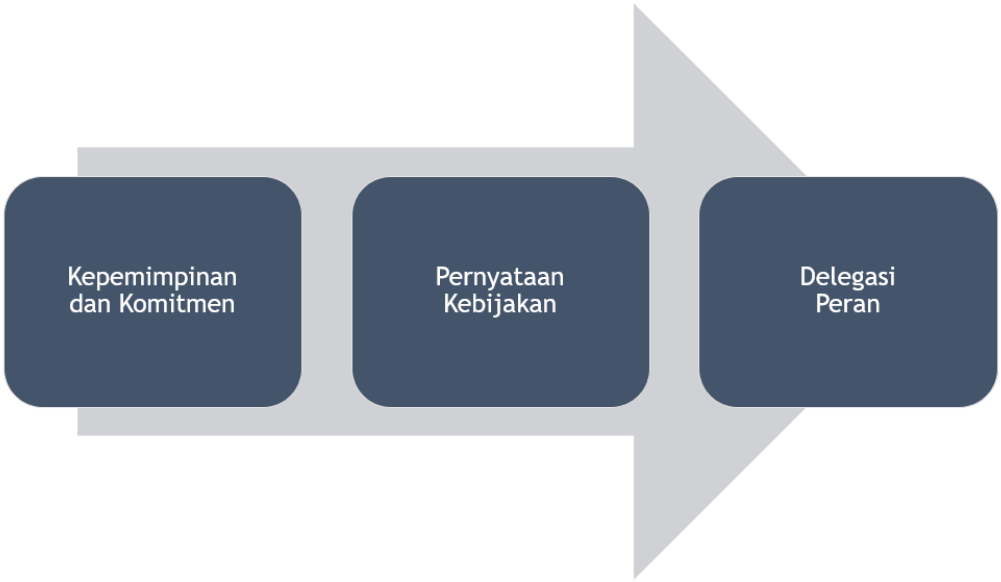
Berdasarkan klausul 5.1 Kepemimpinan dan Komitmen dalam SNI ISO/IEC 27001:2013 menyebutkan secara eksplisit bahwa manajemen puncak harus menunjukkan kepemimpinan dan komitmen terkait SMKI dengan cara:

a. memastikan kebijakan keamanan informasi dan sasaran keamanan informasi ditetapkan dan selaras dengan arah strategis organisasi;
b. memastikan persyaratan SMKI terintegrasi ke dalam proses organisasi;
c. memastikan tersedianya sumber daya yang dibutuhkan untuk SMKI;
d. mengomunikasikan pentingnya manajemen keamanan informasi yang efektif dan kesesuaian dengan persyaratan SMKI;
e. memastikan bahwa SMKI mencapai manfaat yang diharapkan;
f. memberikan arahan dan dukungan pada personel untuk berkontribusi dalam efektivitas SMKI;
g. mempromosikan perbaikan berkelanjutan; dan
h. mendukung peran manajemen yang relevan lainnya untuk menunjukkan kepemimpinannya ketika diterapkan pada wilayah tanggung jawabnya

Selanjutnya, Komitmen manajemen puncak didokumentasikan dalam bentuk pernyataan tertulis berbentuk kebijakan/manual/panduan mutu. Kebijakan itu harus disediakan dalam bentuk informasi terdokumentasi, dikomunikasikan ke seluruh organisasi dan disediakan untuk pihak berkepentingan. Sesuai klausul 5.2 Kebijakan di dalam SNI ISO/IEC 27001:2013, Manajemen puncak harus menetapkan kebijakan keamanan informasi yang:

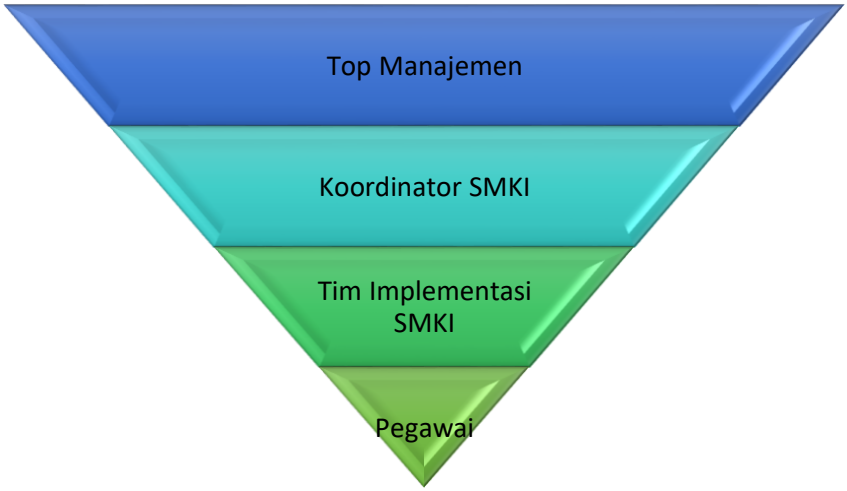
a. sesuai dengan tujuan organisasi;
b. mencakup sasaran keamanan informasi atau menyediakan kerangka kerja untuk menetapkan sasaran keamanan informasi;
c. mencakup komitmen untuk memenuhi persyaratan yang berlaku terkait dengan keamanan informasi; dan
d. mencakup komitmen untuk perbaikan berkelanjutan terhadap SMKI.

Setelah menuangkan pernyataan kebijakan, manajemen puncak mendelegasikan peran, tanggung jawab, dan wewenang dalam penerapan sistem manajemen keamanan informasi. Delegasi itu dilakukan untuk memastikan pemenuhan semua persyaratan sistem manajemen dan pelaporan kinerja kepada manajemen puncak. Informasi terdokumentasi untuk hal tersebut biasanya diwujudkan dalam bentuk uraian tugas (tupoksi) untuk tiap peran (struktural atau fungsional) yang terlibat dalam penerapan sistem manajemen. Manajemen puncak harus memastikan bahwa tanggung jawab dan wewenang untuk peran-peran yang relevan dengan keamanan informasi ditetapkan dan dikomunikasikan. Uraian tugas berupa tanggung jawab dan wewenang itu dapat dicantumkan pada pedoman sistem manajemen atau dokumen lain .Elemen kepemimpinan dalam sistem manajemen dapat terlihat prosesnya pada Gambar dibawah ini dimana hal ini sesuai dengan klausul 5 di standar SNI ISO/IEC 27001:2013.



GAMBAR 4. ELEMEN KEPEMIMPINAN SISTEM MANAJEMEN

Berikut ini merupakan komposisi pembagian peran dalam kepemimpinan didalam suatu sistem manajemen keamanan informasi dimana peran manajemen puncak memiliki proporsi terbesar dalam suatu sistem manajemen khususnya SMKI yang tergambar pada Gambar 3 di bawah ini. Hal ini menunjukkan pentingnya suatu komitmen manajemen puncak dalam hal implementasi sistem manajemen keamanan informasi dalam suatu organisasi. Jika komitmen pimpinan hanya berjalan parsial bahkan tidak ada, maka tidak diragukan lagi implementasi SMKI tidak akan berjalan dengan baik bahkan gagal.



GAMBAR 5. PERAN DALAM KEPEMIMPINAN

9.2 PEMBENTUKAN TIM

Karakteristik dari tim kerja yang efektif yaitu memiliki tujuan serta sasaran yang dipahami dan disetujui oleh semua anggota, konflik dapat diselesaikan, adanya peran yang jelas antar anggota, masing-masing anggota memahami peran, tanggung jawab dan batasan wewenang, adanya evaluasi secara teratur akan proses dan fungsi mereka, dapat memecahkan masalah dan mengambil keputusan, setiap anggota mendukung prosedur dan kontrol tim, digunakannya kemampuan masing-masing anggota tim, adanya rasa kepercayaan dan komunikasi yang terbuka antar anggota (Stott & Walker, 2003). Pembentukan tim dengan pembagian tugas dan tanggung jawab yang tepat merupakan salah satu kunci keberhasilan juga dalam implementasi SMKI dalam suatu organisasi terutama jika pembagian tugas dan tanggung jawab terhadapa SMKI juga berhubungan erat dengan tupoksi anggota tim sehingga sasaran kinerja pegawai para anggota tim juga terpenuhi.

Pembentukan tim yang dimaksud dalam hal ini tidak harus selalu pembentukan tim secara khusus di luar jabatan anggota tim. Namun, penyusunan tim SMKI juga bisa dilakukan dengan menyertakan pengesahan tupoksi jabatan berdasarkan dokumen OTK (Organisasi dan Tata Kelola) suatu organisasi. Sebagai contoh di Badan Standardisasi Nasional tidak dibentuk secara khusus tim SMKI namun menjadikan satu unit yang terlibat dalam ruang lingkup SMKI yaitu seluruh anggota dan pimpinan Pusat Data dan Sistem Informasi BSN menjadi suatu tim SMKI dengan peran dan tanggung jawab yang jelas sesuai dengan jabatan masing-masing anggota tim yang melekat. Hal ini mempermudah baik dalam proses perencanaan maupun implementasi SMKI di lingkungan organisasi BSN.

Namun, penyusunan tim secara khusus yang disahkan dalam suatu Surat Keputusan Manajemen Puncak Organisasi pun diperbolehkan jika sesuai dengan kepentingan organisasi yang bersangkutan dan tidak memberatkan para anggotanya karena bentuk kebijakan yang terlampau ideal dan tidak sesuai dengan kondisi asli suatu organisasi pada akhirnya hanya akan memberatkan

para penerap SMKI di organisasi tersebut sehingga implementasi SMKI tidak dapat berjalan dengan baik.

9.3 PENENTUAN RUANG LINGKUP, GAP ANALISIS, PENGKAJIAN RISIKO DAN SASARAN KEAMANAN INFORMASI

9.3.1 RUANG LINGKUP

Suatu organisasi harus menentukan batasan dan penerapan SMKI dalam menentukan ruang lingkup SMKI dengan mempertimbangkan beberapa hal sebagai berikut :

a. Masalah eksternal dan internal yang relevan dengan tujuan dan yang mempengaruhi kemampuannya untuk mencapai hasil yang diharapkan dari SMKI organisasi;
b. Pihak yang berkepentingan yang relevan dengan SMKI;
c. Persyaratan pihak yang berkepentingan ini yang terkait dengan keamanan informasi;
d. Antarmuka dan ketergantungan antara kegiatan yang dilakukan oleh organisasi, dan kegiatan yang dilakukan oleh organisasi lain.

Penentuan ruang lingkup dalam proses impelementasi SMKI dalam suatu organisasi meliputi :

a. Proses dan/atau Kegiatan. Misalnya: Penyediaan layanan publik, Pengamanan Pusat Data, pengembangan aplikasi, penggunaan jaringan dan fasilitas email, dan sebagainya.
b. Satuan Kerja. Misalnya: Direktorat, Departemen atau Bidang.
c. Lokasi kerja. Misalnya: Tingkat Pusat, daerah atau keduanya.

Penetapan ruang lingkup ini harus didiskusikan dengan Satuan Unit Kerja terkait dengan memperhatikan tingkat kesiapan masing-masing termasuk ketersediaan sumber daya yang diperlukan untuk membangun dan menerapkan SMKI. Selain itu, ruang lingkup yang sudah diputuskan harus terdokumentasi dengan baik.

9.3.2 GAP ANALISIS

Kegiatan ini dilakukan dengan tujuan utamanya untuk membandingkan seberapa jauh persyaratan klausul-klausul SNI ISO/IEC 27001 telah dipenuhi, baik pada aspek kerangka kerja (kebijakan dan prosedur) maupun aspek penerapannya. Untuk aspek kerangka kerja, identifikasilah apakah kebijakan dan prosedur sebagaimana dicantumkan dalam klausul 5.2 telah dipenuhi. Sedang untuk aspek penerapan, periksalah ketersediaan rekaman sebagai bukti-bukti penerapan.

Gap Analysis umumnya dilakukan dengan bantuan checklist pemeriksaan. Selain Checklist Indeks KAMI, checklist lain untuk kegiatan gap analysis ISO 27001 dapat diunduh dari berbagai situs tentang keamanan informasi. Bentuk gap analysis yang paling sederhana berbentuk Cross Reference (CR) dengan membandingkan antara klausul-klausul standar, kontrol dan prosedur-prosedur yang dimiliki terkait SMKI.

Hasil akhir dari gap analysis ini bisa digunakan untuk mengidentifikasi kesiapan suatu organisasi dalam menerapkan SMKI berdasarkan ketersediaan dokumen SMKI-nya. Ada sudut pandang yang harus diperhatikan pada saat penggunaan model CR dalam proses penyusunan gap analysis , yaitu :

a. Jika suatu organisasi sudah memiliki prosedur/dokumen terkait pelaksanaan sistem manajemen keamanan informasi kita sudah punya prosedur/dokumen lalu akan menerapkan standar, maka organisasi tersebut dapat menggunakan model CR ini dalam proses gap analysis dengan mengisikan prosedur/dokumen mana saja yang sudah dimiliki oleh organisasi terkait yang sesuai dengan klausul-klausul standar maupun kontrol kendali di dokumen Lampiran Annex A.
b. Jika suatu organisasi belum memiliki prosedur/dokumen terkait pelaksanaan sistem manajemen keamanan informasi kita sudah punya prosedur/dokumen lalu akan menerapkan standar, maka organisasi tersebut dapat menggunakan model CR ini dalam proses gap analysis dengan mengisikan prosedur/dokumen mana saja yang belum dimiliki oleh organisasi terkait yang sesuai dengan klausul-

klausul standar maupun kontrol kendali di dokumen Lampiran Annex A.

Setelah gap analysis terbentuk, maka selanjutnya proses pengerjaan dokumentasi statement of applicability (SOA) bisa dilakukan. Statement of applicability (SOA) merupakan salah satu dokumen penting saat implementasi dan sertifikasi standar SNI ISO/IEC 27001:2013. Dokumen ini berisi pernyataan organisasi terhadap penerapan kontrol informasi dimana terdapat keterangan yang menyatakan bahwa ada / tidaknya kontrol informasi yang digunakan/diterapkan . Dokumen ini berbentuk checklist pernyataan lingkup penerapan dari 114 kontrol sesuai Annex A SNI ISO/IEC 27001:2013. Berikut ini salah satu contoh bentuk dokumen SOA yang ditunjukkan pada Gambar dibawah ini.

Pernyataan Penerapan

Tanda (untuk Pemilihan Kontrol dan Alasan Pemilihan Kontrol)
PH: Persyaratan Hukum, **KK**: Kewajiban Kontrak, **PB/BP**: Persyaratan Bisnis/Best Practice, **HPR**: Hasil Penilaian Risiko, **SBT**: Sampai Batas Tertentu

Kontrol ISO/IEC 27001:2013			Kontrol saat ini	Catatan Pengecualian	Pemilihan kontrol dan alasan pemilihan				Catatan Penerapan
					PH	KK	PB/BP	HPR	
Clause	Sec	Sasaran Kontrol							
4 Konteks Organisasi	4,1	Konteks Organisasi untuk Keamanan Informasi							
	4.1.1	Identifikasi Isu Internal dan eksternal	Sudah					V	
	4.1.2	Kebutuhan dan ekspetasi Keamanan Informasi	Sudah					V	
	4.1.3	Ruang Lingkup Keamanan Informasi	Sudah					V	
5 Kebijakan Keamanan Informasi	5,2	Arahan Manajemen untuk Keamanan Informasi							
	5.2.1	Kebijakan untuk Keamanan Informasi	Sudah		V				
	5.2.2	Review Kebijakan Keamanan Informasi	Belum			V			
	5,3	Organisasi Internal							
	5.3.1	Aturan Keamanan Informasi dan Tanggung Jawab	Sudah		V				
	5.3.2	Pemisahan Tugas	Sudah				V		
	5.3.3	Hubungan dengan Otoritas	Partial				V		
	5.3.4	Hubungan dengan Unit terkait	Partial				V		
	5.3.5	Keamanan Informasi dalam Manajemen Proyek	Partial			V			

GAMBAR 6. CONTOH BENTUK DOKUMEN STATEMENT OF APPLICABILITY (SOA)

9.3.3 PENGKAJIAN RISIKO

Suatu organisasi dalam melakukan proses implementasi SMKI harus mempertimbangkan permasalahan eksternal maupun internal yang relevan dan persyaratan pihak-pihak yang berkepentingan seperti persyaratan hukum dan peraturan perundang undangan, serta kewajiban kontraktual serta menetukan risiko dan peluang yang perlu ditangani yang bertujuan untuk :

a. memastikan SMKI dapat mencapai manfaat yang diharapkan;

b. mencegah, atau mengurangi, efek yang tidak diinginkan;
c. mencapai perbaikan yang berkelanjutan.

Selain itu, berdasarkan klausul 6.1, suatu organisasi harus merencanakan tindakan untuk menangani risiko dan peluang serta bagaimana cara mengintegrasikan dan menerapkan tindakan ke dalam proses SMKI serta mengevaluasi tindakan tersebut.

Sebelum melakukan risk assessment (pengkajian risiko), metodologi risk assessment harus ditetapkan terlebih dahulu. Metodologi risk assessment TIK harus merujuk pada metodologi risk assessment yang ditetapkan di tingkat pusat, jika sudah ada. Jika belum ada metodologi risk assessment, lakukan penyusunan metodologinya dengan merujuk pada standar standar yang ada, baik standar nasional ataupun internasional. Khusus untuk SMKI, dokumen yang digunakan sebagai rujukan untuk pengkajian risiko yangs esuai dengan standar SNI ISO/IEC 27001:2013 yaitu dokumen SNI ISO/IEC 27001:2013 terkait Manajemen Risiko Keamanan Informasi dan dokumen SNI ISO/IEC 31000:2018 terkait Sistem Manajemen Risiko.

Dalam metodologi risk assessment juga terdapat kriteria penerimaan risiko, dimana risiko yang berada pada tingkat tertentu (umumnya tingkat “RENDAH”) akan diterima tanpa perlu melakukan rencana penanggulangan (Risk Treatment Plan). Risk Assessment dilakukan dengan merujuk pada metodologi yang telah ditetapkan tersebut. Hasil akhir dari proses pengkajian risiko ini berbentuk dokumen Risk Register/Matriks Risiko.

9.3.4 SASARAN KEAMANAN INFORMASI

Berdasarkan klausul 6.2 SNI ISO/IEC 27001:2013, organisasi harus menetapkan sasaran keamanan informasi pada fungsi dan tingkatan yang relevan dengan persyaratan sebagai berikut :

a. konsisten dengan kebijakan keamanan informasi;
b. dapat diukur (jika dapat diterapkan);
c. mempertimbangkan persyaratan keamanan informasi yang berlaku, dan hasil dari penilaian risiko dan penanganan risiko;
d. dikomunikasikan; dan
e. diperbarui jika diperlukan

Ketika merencanakan bagaimana mencapai sasaran keamanan informasinya, organisasi harus menetapkan:

a. apa yang akan dilakukan;
b. sumber daya apa yang akan diperlukan;
c. siapa yang akan bertanggung jawab;
d. kapan akan selesai; dan
e. bagaimana hasilnya akan dievaluasi.

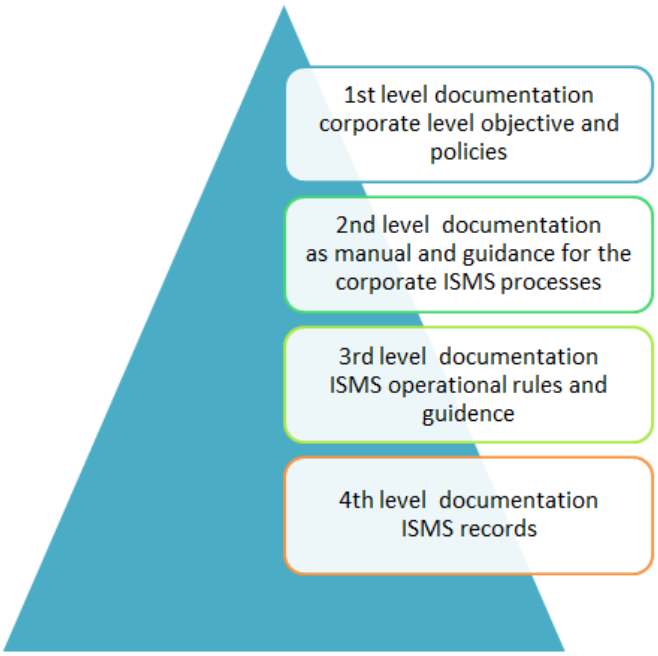
Sasaran keamanan informasi tahunan yang digunakan sebagai patokan untuk mengukur efektivitas penerapan SMKI pada periode yang ditetapkan berdasarkan dokumen SOA dan risk register. Sasaran keamanan informasi tahunan dapat ditetapkan sesuai hasil kajian risiko dan prioritas pembenahan dengan mempertimbangkan ketersediaan dan kemampuan sumber daya.

9.4 PELATIHAN ANGGOTA TIM

Berdasarkan klausul 7 standar SNI ISO/IEC 27001:2013, Organisasi harus menentukan dan menyediakan sumber daya yang dibutuhkan untuk penetapan, penerapan, pemeliharaan dan perbaikan berkelanjutan terhadap SMKI. Setelah menentukan sumber daya yang dibutuhkan, selanjutnya organisasi juga harus menentukan kompetensi yang diperlukan untuk personel yang melakukan pekerjaan di bawah kendali organisasi yang mempengaruhi kinerja keamanan informasi organisasi, memastikan bahwa personel ini kompeten berdasarkan pendidikan, pelatihan, atau pengalaman yang sesuai, apabila memungkinkan, mengambil tindakan untuk memperoleh kompetensi yang diperlukan, dan mengevaluasi efektivitas tindakan yang diambil dan menyimpan informasi terdokumentasi yang sesuai (sertifikat pelatihan) sebagai alat bukti kompetensi. Tindakan peningkatan kompentensi sumber daya manusia suatu organisasi bisa dilakukan dengan penyediaan pelatihan, bimbingan, atau penugasan kembali terhadap karyawan yang ada atau merekrut atau mengontrak personel yang kompeten.

9.5 PENYUSUNAN DOKUMENTASI

Proses penyusunan dokumentasi sistem manajemen keamanan informasi merujuk pada dokumen ISO/ TR 10013:2001 Guidelines for quality management system documentation dimana struktur dokumentasi memiliki tingkatan-tingkatan yang dapat dilihat pada Gambar di bawah ini.



GAMBAR 7. STRUKTUR DOKUMENTASI SISTEM MANAJEMEN KEAMANAN INFORMASI

9.6 SOSIALISASI KE INTERNAL ORGANISASI

Seluruh kebijakan dan prosedur yang telah disetujui oleh pimpinan kemudian disosialisasikan kepada seluruh personel/karyawan yang terkait sesuai dengan ruang lingkup yang ditetapkan di atas. Kegiatan ini untuk menjamin bahwa kebijakan dan prosedur SMKI telah dipahami sehingga penerapannya dilakukan secara tepat. Sosialisasi dapat dilakukan dengan berbagai cara, seperti:

a. Tatap muka di dalam kelas
b. Simulasi langsung di lokasi kerja

c. Penyampaian brosur, leaflet, spanduk untuk meningkatkan kepedulian karyawan.
d. Penggunaan email, nota dinas, portal atau majalah internal.
e. Media komunikasi lainnya

9.7 IMPLEMENTASI

Setelah melakukan sosialiasi secara bertahap pada seluruh internal organiasi, tahap selanjutnya yaitu proses implementasi SMKI berdasarkan ruang lingkup yang telah ditetapkan. Strategi penerapan/implementasi SMKI sebaiknya dilakukan dengan menyelaraskan kegiatan yang sedang berlangsung di instansi/lembaga. Hasil penerapan SMKI harus dicatat dalam bentuk laporan, log, rekaman atau isian formulir yang relevan yang mendukung kebijakan atau prosedur yang ditetapkan seperti laporan pencatatan insiden dan penyelesaiannya, daftar pengguna aplikasi, log aktivitas user, laporan pelatihan/sosialisasi, permintaan perubahan dan realisasinya, hasil pengujian aplikasi, laporan perawatan komputer, dan sebagainya.

9.8 AUDIT INTERNAL

Berdasarkan klausul 9.2 SNI ISO/IEC 27001:2013, Organisasi harus melakukan audit internal pada selang waktu terencana untuk memberikan informasi apakah SMKI sesuai dengan persyaratan yang ditetapkan organisasi untuk SMKI-nya dan persyaratan standar SNI ISO/IEC 27001:2013 dan diimplementasikan dan dipelihara secara efektif. Organisasi juga harus merencanakan, menetapkan, menerapkan dan memelihara program audit, termasuk frekuensi, metode, tanggung jawab, persyaratan perencanaan dan pelaporan. Program audit harus mempertimbangkan pentingnya proses yang bersangkutan dan hasil audit sebelumnya. Selain itu organisasi juga harus menentukan kriteria audit dan ruang lingkup untuk setiap audit, lalu memilih auditor dan melakukan audit yang menjamin objektivitas dan ketidakberpihakan proses audit, memastikan bahwa hasil audit tersebut dilaporkan kepada manajemen yang relevan dan menyimpan informasi terdokumentasi sebagai alat bukti dari program audit dan hasil audit.

Audit internal dilakukan untuk menjamin agar penerapan SMKI dilakukan secara tepat sesuai dengan kebijakan dan prosedur yang ditetapkan. Audit internal harus dilakukan oleh personel/tim yang memiliki kompetensi di bidang audit TIK dan tidak melaksanakan kegiatan yang diaudit. Personel/tim yang melakukan audit internal harus ditetapkan oleh pimpinan/pejabat yang berwenang melalui Surat Keputusan atau Surat Penugasan yang resmi. Audit internal dapat dilakukan oleh pihak eksternal yang diminta secara resmi oleh instansi penyelenggara pelayanan public.

9.9 KAJI ULANG MANAJEMEN

Berdasarkan klausul 9.3 Reviu Manajemen, manajemen puncak harus mereviu organisasi SMKI pada selang waktu terencana untuk memastikan kesesuaian, kecukupan dan efektivitas. Proses reviu manajemen harus mencakup beberapa pertimbangan, yaitu :

a. status tindakan dari reviu manajemen sebelumnya;
b. perubahan isu eksternal dan internal yang relevan dengan SMKI;
c. umpan balik dari kinerja keamanan informasi, termasuk kecenderungan dalam hal:
    - ketidaksesuaian dan tindakan korektif;
    - hasil pemantauan dan pengukuran;
    - hasil audit; dan
    - pemenuhan terhadap sasaran keamanan informasi;
d. umpan balik dari pihak yang berkepentingan;
e. hasil penilaian risiko dan status rencana penanganan risiko; dan
f. peluang untuk perbaikan berkelanjutan

Implementasi seluruh kebijakan, prosedur atau standar yang ditetapkan kemudian dievaluasi efektivitasnya. Hasil pengukuran efektivitas kontrol dan laporan audit internal juga dievaluasi untuk diperiksa mana kontrol yang belum mencapai sasaran, masih lemah (belum efektif) atau yang masih menjadi temuan dalam audit internal. Seluruh kelemahan kontrol harus segera diperbaiki ataupun disempurnakan sehingga tidak menimbulkan kelemahan/kesalahan yang sama di kemudian hari. Keluaran dari reviu manajemen harus mencakup

keputusan yang berkaitan dengan peluang perbaikan berkelanjutan dan setiap kebutuhan untuk perubahan SMKI.

Jika terjadi ketidaksesuaian terhadap hasil audit internal, maka organisasi harus bereaksi terhadap ketidaksesuaian, dan jika dapat diterapkan organisasi akan mengambil tindakan untuk mengendalikan dan mengoreksinya dan menangani konsekuensinya. Selain itu organisasi juga harus mengevaluasi kebutuhan tindakan untuk menghilangkan penyebab ketidaksesuaian, agar hal itu tidak terulang atau terjadi di tempat lain, dengan cara mereviu ketidaksesuaian dan menentukan penyebab ketidaksesuaian serta menentukan apakah ada ketidaksesuaian serupa, atau berpotensi terjadi kembali. Organisasi juga harus melaksanakan tindakan apapun yang diperlukan, mereviu efektivitas tindakan korektif apapun yang diambil dan melakukan perubahan pada SMKI jika diperlukan.

BAB X

PROSES SERTIFIKASI SNI ISO/IEC 27001

10.1 KONSEP SERTIFIKASI

Sertifikasi Sistem Manajemen Keamanan Informasi merupakan sertifikasi terhadap organisasi yang menerapkan sistem manajemen keamanan informasi yang dilakukan oleh lembaga sertifikasi sistem manajemen keamanan informasi yang telah terakreditasi oleh Komite Akreditasi Nasional (KAN). Tujuan dari kegiatan ini adalah terujinya implementasi sistem manajemen keamanan informasi, baik efektifitasnya maupun kesesuaiannya terhadap persyaratan SNI ISO/IEC 27001:2013. Proses sertifikasi dilakukan dengan tahapan sertifikasi awal dan proses surveillance (peninjauan kembali). Untuk proses sertifikasi awal dilakukan dengan dua tahap proses audit yaitu :

a. Audit stage 1 berupa audit kesiapan dokumentasi SMKI. Jika hasil dari audit stage 1 ini menyatakan organisasi penerap SMKI layak untuk melakukan proses sertifikasi maka bisa melanjutkan ke tahap audit selanjutnya. Namun, jika hasil audit stage ini menyatakan organisasi belum siap, maka proses akan berhenti dan organisasi penerap SMKI akan gagal memperoleh sertifikasi.
b. Audit stage 2 berupa audit secara keseluruhan dengan audit terhadap dokumentasi smki, audit rekaman dan wawancara penerapan SMKI.

Organisasi yang mengajukan sertifikasi ISO harus diaudit berdasarkan sampel acak dari lokasi, layanan, fungsi, produk & prosesnya. Tim auditor lembaga sertifikasi akan mencatatkan penyimpangan kepada manajemen. Menurut tingkat penyimpangan, lembaga sertifikasi menentukan waktu yang diperlukan untuk penutupannya termasuk koreksi dan tindakan korektif yang disetujui oleh lembaga sertifikasi. Setelah penutupan ketidaksesuaian / penyimpangan yang efektif oleh organisasi, Sertifikat telah diterbitkan membatasi ruang lingkup yang diaudit. Untuk proses peninjauan kembali proses sertifikasi (surveilance) yang telah diperoleh oleh suatu organisasi dilakukan setiap enam bulan atau satu tahun sekali.

10.2 LEMBAGA SERTIFIKASI SISTEM MANAJEMAN KEAMANAN INFORMASI

Lembaga sertifikasi sistem manajemen keamanan informasi merupakan lembaga yang melakukan proses sertifikasi sistem manajemen keamanan informasi terhadap organisasi yang menerapkan sistem manajemen keamanan informasi yang telah terakreditasi oleh Komite Akreditasi Nasional (KAN). Acuan standar yang digunakan oleh lembaga sertifikasi SMKI dalam melakukan sertifikasi SMKI yaitu :

a. SNI ISO/IEC 17021-1:2015 Penilaian Kesesuaian – Persyaratan lembaga penyelenggara audit dan sertifikasi sistem manajemen – Bagian 1.
b. ISO/IEC 27006:2015 (Information Technology – Security Techniques-Requirement for Bodies Providing Audit and Certification of Information Security Management).
c. Dokumen Pendukung Lembaga Sertifikasi (DPLS) 12

10.3 CRITICAL SUCCESS FACTOR DALAM IMPLEMENTASI SISTEM MANAJEMEN KEAMANAN INFORMASI

Variabel kunci (key variable) atau sering dinamakan sebagai key success factors, key result factors, atau pulse point adalah variabel yang mendefinisikan faktor-faktor yang menjadi penyebab kesuksesan organisasi. Variabel-variabel tersebut merupakan variabel-variabel penting dalam lingkungan internal maupun lingkungan eksternal perusahaan yang sangat mempengaruhi kesuksesan perusahaan dalam melaksanakan strategi untuk mencapai tujuan dan setiap perusahaan harus memberikan perhatian terhadap faktor-faktor tersebut. Terdapat beberapan critical success factors dalam mengimplementasikan sistem manajemen keamanan informasi berbasis SNI ISO/IEC 27001:2013, yaitu :

1. Komitmen dan kepemimpinan dari manajemen puncak;
2. Kebijakan dan sasaran keamanan informasi yang efektif;
3. Pengolaan risiko keamanan informasi yang efektif;

4. Mengimplementasikan dan mengoperasikan SMKI;
5. Menetapkan tugas, tanggung jawab dan kewenangan untuk SMKI;
6. Pelatihan, Awareness, dan kompetensi dari SDM yang efektif;
7. Pengelolaan dokumentasi SMKI yang terstruktur dengan baik;
8. Pengelolaan insiden, kejadian, dan kelemahan keamanan informasi;
9. Internal Audit yang efektif;
10. Peningkatan yang berkelanjutan;
11. Partisipasi aktif organisasi secara keseluruhan;
12. Tinjauan manajemen yang efektif;
13. Pengelolaan motivasi yang efektif;
14. Pengelolaan pengetahuan

BAB XI

PENUTUP

SNI ISO/IEC 27001:2013 adalah kerangka kerja manajemen untuk perlindungan informasi penting bisnis. Bukan standar teknis yang menjelaskan ISMS secara detail teknis. SNI ISO/IEC 27001:2013 juga tidak fokus pada TI (Teknologi Informasi) saja, tetapi juga aset bisnis lain yang penting, sumber daya, dan proses dalam organisasi. Pengelolaan keamanan sistem informasi harus dimulai ketika sebuah sistem informasi dibangun, bukan hanya sebagai pelengkap sebuah sistem informasi.

Struktur SNI ISO/IEC 27001:2013 terdiri dari 10 klausul dan lampiran Anex. Klausul 4 -10 tidak dapat dikecualikan dalam sertifikasi SNI ISO/IEC 27001:2013. Kebutuhan utama SNI ISO/IEC 27001:2013 dibentuk dalam sebuah siklus SMKI. Siklus tersebut terdiri dari *Plan – Do – Check – Act* (PDCA *Cycle*). Klausul yang termasuk dalam ‘Plan’ ialah Organisasi (klausul 4), Kepemimpinan (klausul 5), Perencanaan (klausul 6) dan Dukungan (klausul 7). Klausul yang termasuk dalam ‘Do’ ialah Operasi (klausul 8). Klausul yang termasuk dalam ‘Check’ ialah Evaluasi Kinerja (klausul 9). Klausul yang termasuk dalam ‘Act’ ialah Perbaikan (klausul 10). Adapun manfaat dari SNI ISO/IEC 27001:2013 ini adalah memastikan informasi hanya dapat diakses oleh pihak yang berkepentingan, menjamin keakuratan dan kelengkapan informasi dan pengolahan informasi, dan menjamin bahwa pengguna yang berwenang dapat mengakses informasi saat dibutuhkan.

DAFTAR PUSTAKA

1) Badan Standarisasi Nasional (2013), *SNI SO/IEC 27001:2013 – Teknologi Informasi –Teknik Keamanan – Sistem Manajemen Keamanan Informasi (ISO/IEC 27001:2013, IDT)*, BSN, Bandung.
2) BCA. 2017. *Penerapan ISO 27001:2013 Sistem Manajemen Keamanan Informasi DCN dan DCO GSIT BCA* di http://fkkp-indonesia.org/wp-content/uploads/2017/12/7.-Paparan-Materi-penerapan-ISO-27001-SMKI-DCO-DCN-GSIT-BCA-OJK-Seminar-Nasional-Kearsipan-5-Desember-2017.pdf (akses 14 Mei 2020)
3) Haryanto, Taofik.2015. Audit Kepatuhan Keamanan Informasi menggunakan Kerangka Kerja ISO/IEC 27001 : Studi Kasus PT. XYZ, 1-132
4) ISMS online. 2020. di https://www.isms.online/iso-27001/ (akses 15 Mei 2020)
5) ISO. 2020. *About Us* di https://www.iso.org/about-us.html (akses 15 Mei 2020)
6) Mauladani, Furqon, dan Daniel Oranova Siahaan. 2018. Perancangan SMKI Berdasarkan SNI ISO/IEC27001:2013 dan SNI ISO/IEC27005:2013 (Studi Kasus DPTSI-ITS). CSRID Journal, 10(1), 56-67.
7) Pemahaman Klausul Persyaratan ISO 9001:2015 di https://wqa-apac.com/pemahaman-klausul-persyaratan-iso-9001-2015/ (akses 17 Mei 2020
8) Pratiwi, Wilda Ayu. 2019. Perencanaan Sistem Manajemen Keamanan Informasi berdasarkan Standar ISO 27001:2013 pada Kominfo Provinsi Jawa Timur). 1-168.
9) PT. Edi Indonesia. 2005. *Pengenalan Standard ISO 27001:2005* di https://docplayer.info/storage/54/33683555/1589521574/qweRUexqtxEyLJkcDr05mQ/33683555.pdf (akses 15 Mei 2020)
10) TUVRheinland. 2019. *ISO 27001:2013 Lead Auditor (NON IRCA)*. Jakarta (ID): TUVRheinland.