


Oleh: MUHAMMAD BAHRUDIN[2] dan FIRMANSYAH[3]
Email: *m.bahrudin@bsn.go.id; firmansyah@bsn.go.id*

Manajemen Keamanan Informasi di Perpustakaan Menggunakan Framework SNI ISO/IEC 27001[1]

Abstrak

Peran perpustakaan dengan berbagai jenis dan ukurannya salah satunya ialah menjadi sumber informasi yang mengelola dan menyebarkannya kepada pengguna. Informasi adalah aset penting bagi kelangsungan hidup perpustakaan dan menjamin kepercayaan penggunanya sehingga harus dikelola dengan baik. Perkembangan tata kelola teknologi informasi sangat berperan dalam pengelolaan, investasi dan penyebaran informasi di perpustakaan. Sehubungan dengan hal tersebut, keamanan informasi kemudian menjadi hal penting yang akan berdampak pada pemberdayaan informasi yang efektif. Kebutuhan untuk menyediakan manajemen keamanan informasi yang memadai di perpustakaan menjadi semakin mendesak seiring penerapan tata kelola teknologi informasi yang semakin masif. Makalah ini membahas topik keamanan informasi, pentingnya melindungi informasi dan akses informasi di perpustakaan menggunakan *framework* SNI ISO/IEC 27001:2013. Standar ini memberikan persyaratan yang harus dipenuhi dalam rangka mengimplementasikan sistem manajemen keamanan informasi pada suatu organisasi secara berkelanjutan. Makalah ini bertujuan untuk meningkatkan kesadaran manajemen perpustakaan untuk mengamankan aset informasi yang dimiliki sehingga dapat diberdayakan sesuai dengan prinsip kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaannya (*availability*). Pentingnya manajemen keamanan informasi di perpustakaan ini tentunya akan bermuara pada kepuasan dan kepercayaan pengguna dalam memanfaatkan sumber daya di perpustakaan.

Kata kunci: *Perpustakaan, sistem manajemen keamanan informasi, SMKI, keamanan informasi, ISO 27001*

Pendahuluan

Dahulu ancaman keamanan informasi yang dihadapi oleh perpustakaan hanya bersifat konvensional seperti pencurian dan vandalisme. Saat ini di era informasi, dimana sumber daya perpustakaan telah banyak beralih ke ranah *cyberspace*[4], ancaman yang dihadapi semakin kompleks terkait dengan kerahasiaan, keutuhan dan ketersediaan informasi (*confidentiality, integrity, availability*). Mulai dari ancaman yang paling umum seperti *malware* sampai ancaman berupa pencurian informasi rahasia dan lain-lain. Ancaman-ancaman ini bisa bersumber dari dalam maupun dari luar. Ancaman-ancaman yang masih bersifat potensial ini setiap saat dapat berubah menjadi serangan nyata apabila kelemahan-kelemahan keamanan yang terdapat pada perangkat keras, perangkat lunak, gedung, bisnis proses, dan lain-lain tidak segera diatasi. Ancaman kejahatan di dunia siber ini memiliki risiko tertangkap sangat kecil sementara akibat kerugian yang ditimbulkan bagi perpustakaan lebih besar.

[1] Makalah pernah dipresentasikan pada acara Seminar dan Knowledge Sharing Kepustakawanan dengan tema "Pengembangan Kompetensi Pustakawan sebagai Mitra Peneliti" kerjasama antara Forum Perpusdokinfo LPNK Ristekdikti dan Pusat Dokumentasi dan Informasi Ilmiah – LIPI di Jakarta pada tanggal 23 Mei 2017

[2] Pustakawan Ahli Pertama Pusat Dokumentasi dan Informasi Standardisasi – Badan Standardisasi Nasional

[3] Pustakawan Ahli Pertama Pusat Dokumentasi dan Informasi Standardisasi – Badan Standardisasi Nasional

American Libraries Magazine (Borman, 2017) mengungkapkan baru-baru ini di 700 komputer milik perpustakaan umum di St. Louis, Missouri ditutup untuk layanan peminjaman dan akses internet oleh *hacker*. Penyerang meminta tebusan US$ 35.000 untuk membuka aksesnya. Namun, pihak perpustakaan menolak dan memutuskan untuk *wipe* hardisk seluruh komputer yang terserang. Di Indonesia juga baru-baru ini tengah dihebohkan dengan penyebaran *ransomware* terbaru yang dikenal dengan nama *Wannacry*, sejenis malware yang menyerang komputer korban dengan cara mengunci atau meng-*encrypt* semua file sehingga tidak bisa diakses kembali. Saat ini serangan *Wannacry* ini telah memakan banyak korban di 99 negara termasuk Indonesia. CNN Indonesia (2017) menyebutkan sistem di RS Harapan Kita dan RS Dharmais telah terserang *ransomware* jenis ini. Bahkan Kementerian Komunikasi dan Informatika telah mengeluarkan siaran pers Nomor 56/HM/KOMINFO/05/2017 tentang Antisipasi terhadap Ancaman Malware Ransomware Jenis Wannacry.

Permasalahan

Berdasarkan fakta di atas, terlihat bahwa ancaman keamanan informasi di dunia *cyber* itu nyata dan manajemen perpustakaan perlu melakukan tindakan pencegahan atau antisipasi terhadap aset informasi yang dimilikinya. Lebih lanjut lagi perlu adanya sistem manajemen keamanan informasi yang dapat digunakan sebagai *framework* dalam pengelolaan informasi di perpustakaan. Oleh karena itu, penulis mengenalkan standar yang dapat digunakan sebagai *framework* bagi manajemen perpustakaan terkait dengan keamanan informasi yaitu "SNI ISO/IEC 27001:2013, Teknologi informasi - Teknik keamanan - Sistem manajemen keamanan informasi – Persyaratan"[5].

Berdasarkan latar belakang di atas, makalah ini bertujuan untuk memberikan kesadaran bagi manajemen perpustakaan mengenai pentingnya manajemen keamanan informasi. Kajian sebelumnya terkait dengan keamanan informasi di perpustakaan telah dilakukan diantaranya oleh Irhamni Ali dengan judul Kejahatan terhadap Informasi (*Cybercrime*) dalam Konteks Perpustakaan Digital (Visi Pustaka, 2012) dan Franindya Purwaningtyas dengan judul Aset Informasi Perpustakaan: Tata Kelola dan Keamanan (Visi Pustaka, 2014). Pada makalah ini, penulis secara spesifik memperkenalkan *framework* yang dapat digunakan untuk sistem manajemen keamanan informasi di perpustakaan yaitu SNI ISO/IEC 27001:2013.

Keamanan Informasi di Perpustakaan

Informasi merupakan aset bagi institusi bisnis dan nonbisnis yang sangat berharga. Kehilangan informasi rahasia dapat menyebabkan rusaknya reputasi dan kerugian finansial yang besar. Oleh karena itu keamanan informasi merupakan kebutuhan bisnis perusahaan dari sekedar untuk memberikan jaminan atas terkelolanya risiko bisnis sampai dengan penciptaan keunggulan bersaing bagi perusahaan. Perpustakaan sebagai lembaga informasi memiliki banyak sumber daya yang perlu diamankan, mulai dari database koleksi, data anggota, data pengunjung dan statistik perpustakaan. National Library of Wales (2017) mengategorikan aset informasinya sebagai berikut:

- informasi terkait dengan tata kelola dan manajemen organisasi;
- informasi terkait dengan bangunan dan perawatannya;
- informasi terkait dengan koleksi perpustakaan, seperti; koleksi fisik, koleksi digital, dan katalog dan metadata; dan
- informasi terkait dengan proyek yang didanai pihak eksternal.

Keamanan informasi merupakan upaya untuk melindungi aset informasi yang dimiliki. Upaya perlindungan tersebut dimaksudkan untuk memastikan keberlanjutan bisnis, meminimalkan risiko yang mungkin terjadi dan memaksimalkan keuntungan yang didapat dari investasi dan kesempatan bisnis. Keamanan bisa dicapai dengan beberapa cara atau strategi yang biasa dilakukan secara simultan atau dilakukan dalam kombinasi satu dengan yang lainnya. Strategi dari keamanan informasi masing-masing memiliki fokus dan di bangun tujuan tertentu sesuai kebutuhan (Sarno & Iffano, 2009). Sedangkan menurut SNI ISO/IEC 27000:2014, *information security is preservation of confidentiality integrity and availability of information.* Jadi, keamanan informasi dapat diartikan sebagai preservasi terhadap kerahasiaan, integritas dan ketersediaan informasi.

Berdasarkan definisi di atas, keamanan informasi terdiri dari perlindungan terhadap aspek-aspek berikut (BSN, 2014):

1. ***Confidentiality*** *is property that information is not made available or disclosed to unauthorized*

individuals, entities, or processes atau 'kerahasiaan' yaitu aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.

2. ***Integrity*** *is property of protecting the accuracy and completeness of assets* atau 'integritas' yaitu aspek yang menjamin bahwa data tidak diubah tanpa ada izin pihak yang berwenang *(authorized)*, menjaga keakuratan dan keutuhan informasi, serta metode prosesnya untuk menjamin aspek *integrity* ini.
3. ***Availability*** *is property of being accessible and usable upon demand by an authorized entity* atau 'ketersediaan' yaitu aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan pengguna yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan jika diperlukan).

Nachtigal (2009, dalam Roesnita, 2012) mengategorikan serangan terkait keamanan informasi berdasarkan; kelas serangan (*classes of attack*), motif penyerang (*motives and objectives of the attackers*), teknis serangan (*attack techniques*) dan dampak serangan (*consequences of attacks*). Selengkapnya dapat dilihat pada Tabel 1. Berikut.

Tabel 1. Kategori Serangan terkait Keamanan Informasi

Attack Categories			
a) Classes of attack	b) Motives and objectives of the attackers	c) Attack techniques	d) Consequences of attacks
• Malware (Viruses, worms, Trojans and Spyware	• Harassment	• Buffer overflow	• Software corruption/modification;
• Denial of service (DoS or DDoS)	• Cyber terrorism	• SQL injection	• Hardware malfunction;
• Social engineering	• Political or industrial net espionage	• Spamming	• Data corruption/modification/exposure/ theft;
• Insider attacks		• Packet sniffing	• Identity theft;
• Impersonation attacks		• Spoofing/masquerade	• Intellectual property theft;
• Hacking		• Abuse of cookies	• Financial loss;
• Exploitation of implementation errors		• Routing table poisoning	• Damage to reputation;
		• Phishing	• National-level infrastructure disaster.
		• SMiShing • vishing; • DNS (Domain Name System)	

(Sumber: Nachtigal, 2009 dalam Roesnita, 2012)

Langkah penting dalam perencanaan keamanan informasi adalah memahami aset mana yang perlu dilindungi oleh perpustakaan dan mengapa perlindungan itu diperlukan. Hal ini tentunya membutuhkan kesadaran jenis ancaman dan kerentanan yang dihadapi oleh aset informasi perpustakaan. Perustakaan sebagai perantara antara pengguna dan sumber informasi, melayani beragam klien dan menuntut untuk bekerjasama dalam memberikan akses kepada seluruh penggunanya. Dengan demikian, perpustakaan harus memiliki mekanisme otentikasi yang efektif untuk memastikan kerahasiaan informasi selama pengumpulan, penyimpanan, pemrosesan dan diseminasi hanya kepada pihak yang berwenang, seperti staf perpustakaan dan anggota terdaftar untuk mencegah kebocoran informasi yang sensitif secara tak sengaja. Beberapa masalah keamanan yang sering dialami perpustakaan terkait kerahasiaan informasi misalnya; 1) privasi data pelanggan; dan 2) risiko penetrasi sistem perpustakaan melalui koneksi internet dan modem yang tidak dijaga atau dari petugas yang menyalahgunakan hak akses mereka (Newby & Cain dalam Roesnita, 2012).

SMKI dan SMPI

Sistem manajemen keamanan informasi (SMKI) atau *information security management system* (ISMS) adalah istilah yang muncul terutama dari SNI ISO/IEC 27001:2013 yang diadopsi dari ISO/IEC 27001:2013 merujuk pada suatu sistem manajemen yang berhubungan dengan keamanan informasi. Konsep utama SMKI untuk suatu organisasi adalah untuk merancang, menerapkan, dan memelihara suatu rangkaian terpadu proses dan sistem untuk secara efektif mengelola keamanan informasi dan menjamin kerahasiaan, integritas, serta ketersediaan aset-aset informasi serta meminimalkan risiko keamanan informasi.

Di Indonesia, pada tanggal 11 April 2016, Menteri Komunikasi dan Informatika mengeluarkan regulasi tentang Sistem Manajemen Pengamanan Informasi. Regulasi tersebut tertuang dalam Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (SMPI). Dalam regulasi tersebut, penerapan sistem manajemen pengamanan informasi (SMPI) oleh penyelenggara sistem elektronik ditujukan untuk pelayanan publik yang meliputi:

1) Institusi penyelenggara negara yang terdiri dari

lembaga negara dan/atau lembaga pemerintahan dan/ atau satuan kerja penyelenggara di lingkungannya;
2) Korporasi berupa Badan Usaha Milik Negara dan/ atau Badan Usaha Milik Daerah dan/atau satuan kerja penyelenggara di lingkungannya;
3) Lembaga independen yang dibentuk berdasarkan undang- undang dan/atau satuan kerja penyelenggara di lingkungannya; dan
4) Badan hukum lain yang menyelenggarakan pelayanan publik dalam rangka pelaksanaan misi negara

Lebih lanjut dijelaskan dalam regulasi tersebut bahwa kategorisasi sistem elektronik berdasarkan asas risiko terdiri atas: a) sistem elektronik strategis; b) sistem elektronik tinggi; dan c) sistem elektronik rendah. Dalam lampiran regulasi, disediakan format untuk melakukan kategorisasi sistem elektronik yang dapat dilakukan secara mandiri (*self assessment*) pada setiap sistem elektronik yang dimilikinya. Secara spesifik dalam regulasi tersebut menyebutkan bahwa sistem elektronik yang masuk kategori strategis dan tinggi harus menerapkan standar SNI ISO/IEC 27001 dan ketentuan pengamanan yang ditetapkan oleh instansi pengawas dan pengatur sektornya. Sementara sistem elektronik yang masuk kategori rendah, harus menerapkan pedoman indeks keamanan informasi. Dengan kata lain, berdasarkan regulasi tersebut seluruh instansi baik pemerintah maupun swasta wajib menerapkan sistem manajemen pengamanan informasi (SMPI).

Kesadaran Keamanan Informasi di Perpustakaan

Keamanan sistem informasi tidak hanya melibatkan kontrol keamanan teknis, namun juga melibatkan kontrol administratif, prosedural dan manajerial (Papagiannakis, Pijl, & Visser, 2011). Cara pengguna dalam menggunakan sistem informasi organisasi memainkan peranan penting dalam menjaga kelangsungan aset informasi perusahaan. Kesadaran keamanan informasi adalah bidang ilmu keamanan yang berhubungan erat dengan faktor manusia mengenai keamanan aset informasi. Pengetahuan yang diperoleh dari dunia pendidikan adalah elemen utama untuk menciptakan kesadaran keamanan informasi. Sehingga kesadaran tersebut muncul dalam diri masing-masing individu.

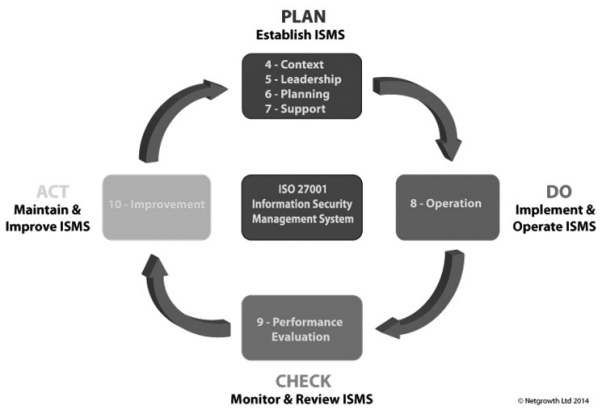
Dhillon dalam Kruger (2011) berpendapat bahwa perilaku informal merupakan dasar untuk menggambarkan karakteristik seseorang, organisasi, dan tindakan komunikasi yang mempengaruhi informasi. Selain itu, dikatakan juga bahwa pola pembelajaran, budaya dan struktur norma yang ada merupakan elemen perilaku informal konstituen. Dengan demikian, dapat disimpulkan bahwa manajemen keamanan informasi hanya dapat dilakukan dengan lengkap jika aspek perilaku individu dan kelompok diketahui. Materi keamanan informasi yang banyak digunakan oleh organisasi saat ini terlalu fokus pada kebijakan keamanan. SAI Global mempunyai filosofi bahwa agar keamanan informasi lebih efektif, maka selain mengatasi pengetahuan pengguna, sangatlah penting untuk mengatasi sikap dan perilaku mereka (SAI Global, 2008). Posisi keamanan organisasi secara keseluruhan dapat ditingkatkan apabila sikap, pengetahuan dan perilaku pengguna sejalan dengan tujuan dan persyaratan keamanan. Sikap pengguna menjadi faktor penting karena selain mereka harus percaya bahwa keamanan sangat penting, pengguna sulit untuk bekerja dengan aman, terlepas dari berapa banyak yang mereka ketahui tetang persyaratan keamanan. Sikap memberikan indikasi yang sangat kuat mengenai arah tindakan karyawan. Pengetahuan penting karena meski-pun pengguna percaya bahwa keamanan itu penting, ia tidak bisa mengubah niat itu menjadi sebuah tindakan tanpa pengetahuan dan pemahaman. Akhirnya, tidak peduli apakah orang percaya atau tahu tentang pentingnya keamanan, hal itu tidak akan memengaruhi keamanan kecuali mereka berperilaku dengan cara yang aman.

Berdasarkan penelitian Amin (2014) menyebutkan bahwa kesadaran keamanan informasi perlu terus ditingkatkan karena keamanan informasi bukan persoalan teknikal saja, tetapi kontribusi kelalaian manusia juga berpengaruh dalam kerentanan keamanan informasi. Kebutuhan perpustakaan terkait keamanan informasi berbanding lurus dengan kesadaran akan relevansi dan pentingnya keamanan informasi di sebuah organisasi. Dalam makalah ini, penulis mengemukakan gagasan dalam rangka kesadaran keamanan informasi bagi manajemen perpustakaan terhadap aset informasi yang dimilikinya dengan implementasi SNI ISO/IEC 27001:2013 terkait SMKI. Hal ini pun selaras dengan regulasi pemerintah dengan adanya Permenkominfo Nomor 4 Tahun 2016 tentang SMPI. Untuk mencapai hal tersebut tentunya diperlukan komitmen manajemen puncak di lingkungan perpustakaan maupun instansi induknya agar implementasi SMKI dapat dilaksanakan secara efektif.

SNI ISO/IEC 27001 untuk Perpustakaan

Dalam rangka manajemen keamanan informasi terhadap aset informasinya, perpustakaan dapat menggunakan *framework* SNI ISO/IEC 27001:2013. Standar ini menentukan persyaratan untuk menetapkan, menerapkan, memelihara dan secara berkelanjutan memperbaiki sistem manajemen keamanan informasi (SMKI) dalam konteks organisasi. Standar ini juga mencakup persyaratan untuk penilaian dan penanganan risiko keamanan informasi disesuaikan dengan kebutuhan organisasi (BSN, 2013). Standar ini mengadopsi "Plan-Do-Check-Act" (PDCA) model yang digunakan untuk mengatur semua proses SMKI. Standar ini juga memberikan model untuk menerapkan prinsip-prinsip dalam pedoman yang mengatur penilaian risiko, desain keamanan dan implementasi, manajemen keamanan dan penilaian ulang. Secara garis besar standar ini menyatakan 7 klausul persyaratan yang harus dipenuhi yaitu:

- konteks organisasi (c*ontext of the organization*),
- kepemimpinan (*leadership*),
- perencanaan (*planning*),
- dukungan (*support*),
- operasi (*operation*),
- evaluasi kinerja (*performance evaluation*), dan
- perbaikan (*improvement*).



Gambar 1. Model PDCA dalam SNI ISO/IEC 27001:2013

(Sumber: netgrowthltd.co.uk)

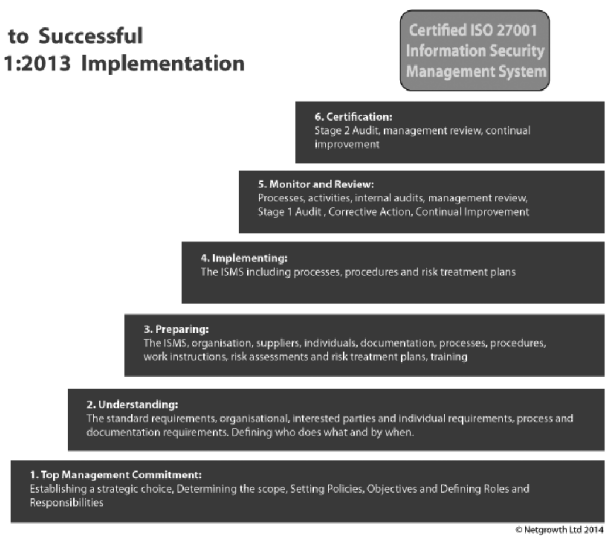
Urutan persyaratan yang disajikan dalam standar tersebut tidak mencerminkan pentingnya persyaratan itu atau dengan kata lain tidak menyiratkan urutan persyaratan yang harus dilaksanakan. Daftar tersebut hanya untuk tujuan referensi. Disamping persyaratan utama, SNI ISO/IEC 27001:2013 menyaratkan penetapan sasaran kontrol dan kontrol keamanan informasi yang meliputi 14 klausul yang di dalamnya termasuk 113 kontrol keamanan informasi. Empat belas klausul tersebut diantaranya sebagai berikut;

- kebijakan keamanan informasi,
- organisasi keamanan informasi,
- sumberdaya manusia menyangkut keamanan informasi,
- manajemen aset,
- akses kontrol,
- kriptografi,
- keamanan fisik dan lingkungan,
- keamanan operasi,
- keamanan komunikasi,
- pengadaan/akuisisi, pengembangan dan pemeliharaan sistem informasi,
- hubungan dengan pemasok,
- pengelolaan insiden keamanan informasi,
- manajemen kelangsungan usaha, dan
- kepatuhan

Bagi manajemen perpustakaan yang memiliki komitmen mengimplementasikan SMKI, standar ini cukup komprehensif untuk dijadikan kerangka kerja (*framework*). Dari 113 kontrol keamanan informasi yang ada dalam standar ini, pada pelaksanaannya manajemen perpustakaan dapat memilih kontrol mana yang paling relevan dengan kondisi di lapangan dengan melakukan penilaian resiko dan aset pada tahapan awal. Pemilihan ini bukan pekerjaan mudah karena banyak parameter yang harus dijadikan pertimbangan. Pada Gambar 2 menunjukkan mengenai 6 (enam) langkah sukses yang dapat dilakukan oleh organisasi, dalam hal ini perpustakaan dalam implementasi SNI ISO/IEC 27001:2013. Selanjutnya selain SNI ISO/IEC 27001 yang berisi persyaratan dan kontrol keamanan informasi terkait SMKI, manajemen juga dapat memanfaatkan referensi seri ISO 27000 lainnya yang sebagian besar telah diadopsi menjadi Standar Nasional Indonesia (SNI), diantaranya:

- SNI ISO/IEC 27000:2014, *Teknologi informasi - Teknik keamanan - Sistem manajemen keamanan informasi - Gambaran umum dan kosakata,*
- SNI ISO/IEC 27002:2013, *Teknologi informasi - Teknik keamanan - Panduan praktik manajemen keamanan informasi*
- SNI ISO/IEC 27002:2014/Corr.1:2016, *Teknologi informasi - Teknik keamanan - Petunjuk praktik*

kendali keamanan informasi (RALAT 1)
- SNI ISO/IEC 27003:2013, *Teknologi Informasi - Teknik keamanan - Panduan implementasi sistem manajemen keamanan informasi*
- SNI ISO/IEC 27004:2013, *Teknologi informasi - Teknik keamanan - Manajemen keamanan informasi - Pengukuran*
- SNI ISO/IEC 27005:2013, *Teknologi informasi - Teknik keamanan - Manajemen risiko keamanan informasi*
- SNI ISO/IEC 27007:2013, *Teknologi Informasi - Teknik keamanan - Pedoman audit sistem manajemen keamanan informasi*
- SNI ISO/IEC TR 27008:2013, *Teknologi Informasi - Teknik keamanan - Pedoman untuk auditor tentang kendali keamanan informasi*
- SNI ISO/IEC 27009:2017, *Teknologi informasi - Teknik keamanan - Penerapan sektor spesifik dari ISO/IEC 27001 – Persyaratan*



Gambar 2. Enam Langkah Sukses Implementasi SNI ISO/IEC 27001:2013
(Sumber: netgrowthltd.co.uk)

Selanjutnya, terkait dengan manfaat implementasi SNI ISO/IEC 27001 di perpustakaan, yaitu agar:
a) Manajemen perpustakaan mampu menerapkan tata kelola keamanan informasi secara efektif, efisien dan konsisten dengan pendekatan berbasis risiko;
b) Manajemen perpustakaan patuh terhadap hukum dan undang-undang seperti UU ITE dan Permenkominfo Nomor 4 Tahun 2014 tentang SMPI;
c) Manajemen perpustakaan mampu melakukan penilaian mandiri (*self assessment*) secara berkala melalui;
d) Manajemen perpustakaan mampu menyusun sistem dokumentasi minimum yang diperlukan untuk menerapkan tata kelola keamanan informasi;
e) Manajemen perpustakaan mampu memberikan pemahaman pentingnya keamanan informasi pada staf, pustakawan, *stakeholder* dan masyarakat umum;
f) Manajemen perpustakaan mengimplementasikan standar pengamanan informasi yang diakui dunia;
g) Meningkatkan kepercayaan pengguna dan seluruh *stakeholder* yang ada terhadap pelayanan yang diberikan perpustakaan;
h) Manajemen perpustakaan dapat mengintegrasikan atau mengombinasikan dengan sistem manajemen lainnya seperti ISO 9000, ISO 14000, COBIT dan lain-lain.

Kendala dalam Implementasi SNI ISO/IEC 27001 di Perpustakaan

Implementasi SNI ISO/IEC 27001 oleh manajemen perpustakaan sangat penting dalam rangka mengamankan aset informasinya. Namun demikian dalam perencanaan maupun pelaksanaannya tentu akan menghadapi berbagai kendala yang bahkan kendala tersebut dapat berdampak pada kegagalan dalam proses implementasi SMKI di perpustakaan. Berikut adalah beberapa kendala yang mungkin dapat dihadapi oleh manajemen perpustakaan dalam implementasi SMKI berdasarkan SNI ISO/IEC 27001.

1) Kendala manajerial

Ketika suatu perpustakaan berkomitmen menerapkan SMKI, dibutuhkan komitmen dari manajemen khususnya tim manajemen yang nantinya terlibat dalam ruang lingkup penerapan SMKI. Hal ini karena tujuan dari implementasi SMKI adalah untuk menyusun suatu sistem manajemen, maka jika tidak ada komitmen dari manajemen, apalagi manajemen puncak, penerapan SMKI di perpustakaan tidak akan berjalan dan berpotensi tinggi mengalami kegagalan. Kurangnya komitmen dari manajemen merupakan faktor utama kegagalan implementasi SMKI. Untuk mengatasi kendala ini, maka perlu untuk membuat kebijakan yang disahkan oleh manajemen terkait penerapan SMKI di perpustakaan. Hal ini akan mengikat dan menuntut komitmen dari seluruh manajemen yang terlibat dalam SMKI.

2) Kendala sumberdaya manusia

Terkait sumber daya manusia, dalam imlementasi SMKI di perpustakaan menjadi kendala karena kurangnya SDM yang mendukung proses tersebut. Kendala terkait SDM ini diantaranya terkait;

a) Kurangnya pemahaman dan kompetensi pegawai/ staf untuk mendukung penerapan SMKI,
b) Kurangnya jumlah personel sehingga menuntut SDM yang ada untuk *multitasking*,
c) Tidak adanya sosialisasi bagi staf perpustakaan terkait implementasi SMKI sehingga kesadaran personel terhadap implementasi tersebut kurang,
d) Tidak adanya personel yang ahli di bidang keamanan informasi di perpustakaan sehingga implementasi yang dilakukan tidak praktis.

Untuk mengatasi kendala tersebut, manajemen perpustakaan perlu memberikan perhatian khusus, semisal mengadakan *awareness* dan/atau pelatihan terkait SNI ISO/IEC 27001.

3) Kendala budaya organisasi

Budaya organisasi juga dapat menjadi kendala dalam melakukan implementasi SMKI. Budaya yang tidak sadar akan pentingnya keamanan informasi, dan telah tertanam sehari-hari tentunya sulit untuk dirubah. Hal tersebut dapat menimbulkan resistensi terhadap perubahan atau penambahan kegiatan baru seperti implementasi SMKI ini. Untuk mengatasi kendala tersebut, manajemen puncak di lingkungan perpustakaan perlu memberikan dukungan penuh terhadap implementasi SMKI dan juga dapat memasukkan proses penerapan SMKI ke dalam sasaran penilaian kinerja tim atau personel untuk mendukung terlaksananya implementasi tersebut.

4) Kendala organisasi

Kurangnya tingkat kematangan organisasi, dalam hal ini manajemen perpustakaan, dalam mengelola proses bisnis/kegiatan dapat menjadi penghambat proses implementasi SMKI. Hal ini seringnya dihadapi oleh organisasi menengah ataupun baru (termasuk hasil adanya reorganisasi) karena belum secara jelas menetapkan tugas dan tanggung jawab pekerjaan atau tugas pokok dan fungsinya (tupoksi). Selain itu perubahan terhadap struktur organisasi dapat menghambat implementasi SMKI, terutama ketika perubahan tersebut terjadi pada saat proses implementasi sedang berjalan. Untuk mengatasi kendala tersebut, jika belum ada tupoksi yang jelas, maka dapat dibuat berdasarkan fungsi yang ada pada SNI ISO/IEC 27001. Selain itu, proses implementasi SMKI harus terdokumentasikan secara lengkap agar permasalahan yang terkait perubahan struktur organisasi tidak akan memengaruhi atau menghambat implementasinya.

5) Kendala teknis

Faktor penghambat atau kendala selanjutnya dalam implementasi SMKI ialah kurangnya teknologi informasi yang mendukung. Hal ini dapat terjadi karena minimnya anggaran di perpustakaan atau dapat juga dikarenakan kurang akuratnya estimasi dan pengelolaan anggaran yang telah direncanakan untuk mendukung implementasi SMKI. Untuk mengatasi kendala tersebut, manajemen perpustakaan perlu mengatur penganggaran kembali sesuai dengan kebutuhan, dalam hal ini pengalokasian anggaran untuk mendukung proses implementasi SMKI.

Kesimpulan

Di era perkembangan teknologi informasi dan perpustakaan dewasa ini juga tidak lepas dari dunia digital, urgensi implementasi manajemen keamanan informasi sangat tinggi. Aset-aset informasi di perpustakaan mulai dari data pengguna, koleksi dan manajemen perpustakaan lainnya harus dikendalikan untuk dapat diberdayakan oleh pihak yang berhak (internal dan eksternal). Langkah pengendalian tersebut dapat dilakukan dengan implementasi SMKI dengan *framework* SNI ISO/IEC 27001. Hal ini pun sejalan dengan program regulasi pemerintah melalui Permenkominfo Nomor 4 Tahun 2016 tentang SMPI. Namun demikian, untuk menerapkan SMKI di perpustakaan memang tidaklah mudah. Banyak faktor yang dapat menjadi kendala atau penghambat dalam implementasi SMKI dan bahkan kendala tersebut dapat menimbulkan kegagalan implementasi SMKI. Kendala-kendala tersebut mulai dari terkait dengan manajerial, sumberdaya manusia, budaya organisasi, organisasi itu sendiri dan juga kendala terkait teknis.

Berbagai kendala tersebut kuncinya dapat diatasi mulai dari komitmen manajemen yang dalam hal ini adalah manajemen puncak terkait dengan implementasi SMKI di perpustakaan. Setelah itu, perlu adanya *awareness* kepada sumberdaya manusia yang ada di perpustakaan secara berkelanjutan dan juga melibatkan SMKI dalam kinerja pegawai yang nantinya dapat menjadi budaya

organisasi yang sadar terhadap keamanan informasi. Implementasi SMKI juga harus didokumentasikan secara lengkap untuk mengantisipasi dinamika organisasi. Kemudian yang tidak kalah penting adalah manajemen perlu mengalokasikan anggaran untuk mendukung dan mengakomodir implementasi SMKI di perpustakaan.

Daftar Pustaka

Amin, M. (2014). Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan Multile Criteria Decision Analysis (MCDA). *Jurnal Penelitian dan Pengembangan Komunikasi dan Informatika, 5*(1), 15-24.

Borman, L. D. (2017). *Cybersecurity and Privacy in 2017: ProQuest Midwinter breakfast covers issues and tips*. Diakses 14 Mei 2017, dari American Libraries: https://americanlibrariesmagazine.org/blogs/the-scoop/cybersecurity-privacy-2017/

BSN. (2013). *SNI ISO/IEC 27001:2013, Teknologi informasi - Teknik keamanan - Sistem manajemen keamanan informasi - Persyaratan.* Jakarta: Badan Standardisasi Nasional.

BSN. (2014). *SNI ISO/IEC 27000:2014, Teknologi informasi - Teknik keamanan - Sistem manajemen keamanan informasi - Gambaran umum dan kosakata.* Jakarta: Badan Standardisasi Nasional.

CNN Indonesia. (2017). *RS Dharmais dan Harapan Kita Bebas dari Sandera Ransomware*. Diakses 15 Mei 2017, dari CNN Indonesia: http://www.cnnindonesia.com/teknologi/20170515103955-185-214857/rs-dharmais-harapan-kita-bebas-dari-sandera-ransomware/

IT Governance Indonesia. (2016). *FYI: Telah Terbit Peraturan Menteri Kominfo No. 4 Tahun 2016*. Diakses 14 Mei 2017, dari IT Governance Indonesia: https://itgid.org/fyi-telah-terbit-peraturan-menteri-kominfo-no-4-thn-2016/

Kruger, H. A., Flowerday, S., Drevin, L., & Steyn, T. (2011). *An Assessment of the role of cultural factors in information security awareness.* ISSA.

Papagiannakis, K., Pijl, G. v., & Visser, A. d. (2011). *An Overview of the current level of Security Awareness in Greek Companies.* Erasmus University of Rottersam.

Roesnita. (2012). *Assessing information security management in Malaysian academic libraries.* Malaysia: University of Malaya.

SAI Global. (2008). *Security Awareness: Measuring Attitudes, Knowledge and Behaviour.* SAI Global.

Sarno, R., & Iffano, I. (2009). *Sistem manajemen keamanan informasi berbasis ISO 27001.* Surabaya: ITS Press.

The National Library of Wales. (2017). *List of Information Assets*. Diakses 14 Mei 2017, dari The National Library of Wales: https://www.llgc.org.uk/en/about-nlw/governance/psi-regulations/list-of-information-assets/