STANDAR MANAJEMEN KEAMANAN SISTEM INFORMASI BERBASIS ISO/IEC 27001:2005

Chalifa Chazar

ABSTRAK

Informasi merupakan salah satu aset penting bagi perusahaan. Oleh karena itu kemampuan untuk menyediakan informasi secara cepat dan akurat merupakan hal yang esensial. Pengelolaan informasi sering kali melibatkan peran Sistem Informasi (SI) dan Teknologi Informasi (TI). Akan tetapi seiring perkembangannya, TI seringkali dimanfaatkan oleh beberapa pihak yang tidak bertanggung jawab yang dapat menimbulkan ancaman dan resiko yang dapat merugikan perusahaan. Masalah keamanan seringkali kurang mendapatkan perhatian dari pihak stakeholder. "*Prevention is better than cure*". Seri ISO/IEC 27000 menawarkan satu set spesifikasi, kode etik dan pedoman praktik terbaik (*best practise*) untuk memastikan manajemen layanan TI (Teknologi Informasi) . ISO/IEC 27001 merupakan standar yang sering digunakan untuk mengetahui kebutuhan untuk menerapkan keamanan sistem informasi. Dengan penerapan ISO/IEC 27001 dapat melindungi aspek-aspek dari keamanan informasi yaitu *confidentiality*, *integrity* dan *availability*.

Kata kunci: Keamanan Sistem Informasi, ISMS, SMKI, ISO/IEC 27000, ISO/IEC 27001

1. PENDAHULUAN

Seiring dengan perkembangan laju teknologi, informasi merupakan salah satu aset penting dari perusahaan. Kemampuan untuk menyediakan informasi yang akurat dan cepat menjadi suatu hal yang penting. Dapat dikatakan Sistem Informasi (SI) sudah menjadi sebuah bagian dari perusahaan. SI digunakan untuk mendukung berbagai kegiatan dalam perusahaan, bahkan untuk memperoleh keuntungan dan memenangkan persaingan. SI berkembang seiring perkembangan Teknologi Informasi (TI). Namun, seiring perkembangannya teknologi sering kali dimanfaatkan oleh beberapa pihak yang tidak bertanggungjawab yang dapat menyebabkan munculnya ancaman dan resiko dari penggunaan teknologi.

Masalah keamanan sistem informasi sering kali kurang mendapatkan perhatian dari para stakeholder dan pengelola sistem informasi. Sering kali, permasalahan keamanan sistem informasi mendapatkan perhatian dari para stakeholder dan pengelola sistem informasi ketika sudah terjadi sebuah ancaman yang menimbulkan kerugian pada perusahaan. Ketika sebuah ancaman sudah menimbulkan kerugian pada perusahaan, stakeholder dan pengelola sistem mulai melakukan berbagai tindakan pencegahan dan perbaikan atas keamanan sistem informasi. Hal ini dapat menyebabkan perusahaan

mengeluarkan pengeluaran ekstra untuk melakukan pengamanan sistem informasi dan perbaikan atas ancaman yang sudah terjadi. Apabila menggangu performansi dari sistem, sering kali keamanan dikurangi atau ditiadakan [1].

Prevention is better than cure, mencegah lebih baik dari pada mengobati. Keamanan sistem informasi bertujuan untuk memastikan dan menyakinkan integritas, ketersediaan dan kerahasiaan dari pengolahan informasi. Pengelolaan keamanan sistem informasi harus dimulai ketika sebuah sistem informasi dibangun, bukan hanya sebagai pelengkap sebuah sistem informasi. Dengan adanya pengelolaan keamanan sistem informasi yang baik, maka diharapkan perusahaan dapat memprediksi resiko-resiko yang muncul akibat penggunaan sistem informasi sehingga dapat menghindari atau mengurangi resiko yang mungkin dapat merugikan perusahaan. Keamanan sistem informasi merupakan tanggungjawab semua pihak yang ada di dalam perusahaan.

Oleh karena itu bagaimana perusahaan dapat menerapkan dan mengelola keamanan sistem informasi, melatarbelakangi disusunnya seri ISO/IEC 27000, merupakan standar untuk manajemen keamanan sistem informasi. Seri ISO/IEC 27000 menawarkan satu set spesifikasi, kode etik dan pedoman praktik terbaik (*best practise*) untuk memastikan manajemen layanan TI (Teknologi Informasi) [8]. ISO/IEC 27001 merupakan standar yang sering digunakan untuk mengetahui kebutuhan untuk menerapkan keamanan sistem informasi.

2. PEMBAHASAN MASALAH

2.1 Ancaman Terhadap Sistem Informasi

Ancaman adalah suatu aksi atau kejadian yang dapat merugikan perusahaan [4]. Kerugian bisa berupa uang, tenaga, kemungkinan berbisnis (*business opportunity*), reputasi organisasi bahkan mungkin dapat menyebabkan pailit. Menurut W. Stallings ada beberapa kemungkinan ancaman, yaitu [1]:

1) *Interruption*, perangkat sistem rusak atau menjadi tidak tersedia, merupakan ancaman terhadap aspek *availability* (ketersediaan).
2) *Interception*, pengaksesan informasi oleh pihak yang tidak berwenang.
3) *Modification*, pihak yang tidak memiliki wewenang tidak hanya mengakses informasi tetapi juga melakukan perubahan terhadap informasi.

4) *Fabrication*, penyisipan objek palsu ke dalam sistem oleh pihak yang tidak berwenang.

Berikut ini beberapa kasus yang berhubungan dengan ancaman terhadap keamanan sistem informasi di Indonesia antara lain:

1) Pada Januari 2000, beberapa sistus web di Indonesia diacak-acak oleh cracker yang menamakan dirinya"fabianclone" dan "aisenodni" (Indonesia dibalik). Situs yang diserang termasuk Bursa Efek Jakarta, BCA, Indosatnet, dan beberapa situs besar lain yang tidak dilaporkan [1].
2) September dan Oktober 2000, setelah membobol Bank Lippo, kembali Fabian Clone beraksi dengan menjebol web milik Bank Bali [1].
3) 16 April 2001, Polda DIY meringkus seorang *carder* (pembobol kartu kredit). Tersangka diringkus di Bantul dengan barang bukti sebuah paket berisi lukisan berharga 30 juta rupiah [1].
4) Dikutip dari berita elektronik www.republika.co.id, perubahan kartu tanda penduduk (KTP) menjadi bentuk elektronik (e-KTP), merupakan salah satu contoh sistem yang rentan dalam hal keamanannya, mengingat data yang ada di dalamnya merupakan data rahasia, data privasi yang perlu dilindungi [10].

Menurut David Icove berdasarkan lubang keamanan, keamanan dapat diklasifikasikan menjadi 4, yaitu [1]:

1) Keamanan yang bersifat fisik (*physical security*)
2) Keamanan yang berhubungan dengan orang
3) Keamanan dari data dan media serta teknik komunikasi
4) Keamanan dalam operasi

2.2 Keamanan Sistem Informasi

Keamanan sistem informasi merupakan hal yang perlu mendapat perhatian saat membangun sebuah sistem informasi. Bayangkan kita membuat sebuah rumah yang lengkap dengan jendela dan pintu, tetapi kita tidak membuat kunci untuk pintu dan jendela. Hal ini dapat menyebabkan seseorang bisa dengan mudah memasuki rumah kita, bahkan mungkin melakukan pencurian. Sama halnya dengan membangun sistem informasi, keamanan sistem informasi digunakan untuk menghindari seseorang yang tidak memiliki akses untuk dapat masuk ke dalam sistem.

Menurut G. J. Simons, keamanan sistem informasi adalah bagaimana kita dapat mencegah penipuan (*cheating*) atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik [1]. Menurut John D. Howard dalam bukunya "*An Analysis of Security Incidents on The Internet*" menyatakan bahwa keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab [2].

2.3. Aspek-aspek Terhadap Keamanan Informasi

Informasi merupakan salah satu aset penting dari perusahaan. Perusahaan melakukan pengolahan terhadap informasi, kemudian hasilnya disimpan dan dibagikan. Keamanan sistem informasi terdiri dari perlindungan terhadap aspek-aspek berikut ini:

1) *Confidentiality* (Kerahasiaan)

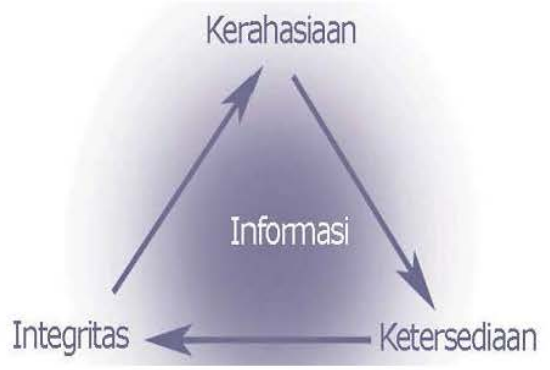
   Aspek yang menjamin kerahasian data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasian data yang dikirim, diterima dan disimpan [3].

2) *Integrity* (Integritas)

   Aspek yang menjamin bahwa data tidak diubah tanpa ada ijin pihak yang berwenang (authorized), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integrity ini [3].

3) *Availability* (Ketersediaan)

   Aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bilamana diperlukan) [3].



Gambar 1. Aspek-Aspek Keamanan Sistem Informasi [3]

Sumber lain menyebutkan bahwa aspek keamanan sistem informasi melingkupi 4 aspek. Grafinkel mengemukakan bahwa keamanan komputer melingkupi 4 aspek, yaitu *privasi*, *integrity*, *authentication* dan *availability* [1]. Selain keempat hal di atas, masih ada dua aspek lain yang juga sering dibahas dalam kaitannya dengan *electronic commerce*, yaitu *access control* dan *non-repudiation* [1].

2.4. Standar Manajemen Keamanan Informasi (SMKI)

Pengelolaan keamanan sistem informasi yang baik dibutuhkan untuk mengantisipasi ancaman-ancaman yang mungkin terjadi. Bagaimana perusahaan dapat menerapkan dan mengelola keamanan sistem informasi, melatarbelakangi disusunnya seri ISO/IEC 27000, merupakan standar tentang *Information Security Management System* (ISMS) atau dikenal juga dengan istilah Sistem Manajemen Keamanan Informasi (SMKI).

Menurut ISO/IEC 27000:2014, ISMS adalah pendekatan sistematis untuk menetapkan, mengimplementasi, operasional, pemantauan, peninjauan, pemelihharaan dan meningkatkan keamanan informasi pada organisasi untuk mencapai tujuan bisnis. Menurut ISO/IEC 27001:2014, keamanan sistem informasi tidak hanya berhubungan dengan penggunaan perangkat lunak antivirus, *firewall*, penggunaan *password* untuk komputer, tetapi merupakan pendekatan secara keseluruhan baik dari sisi orang, proses dan teknologi untuk memastikan berjalannya efektivitas keamanan.

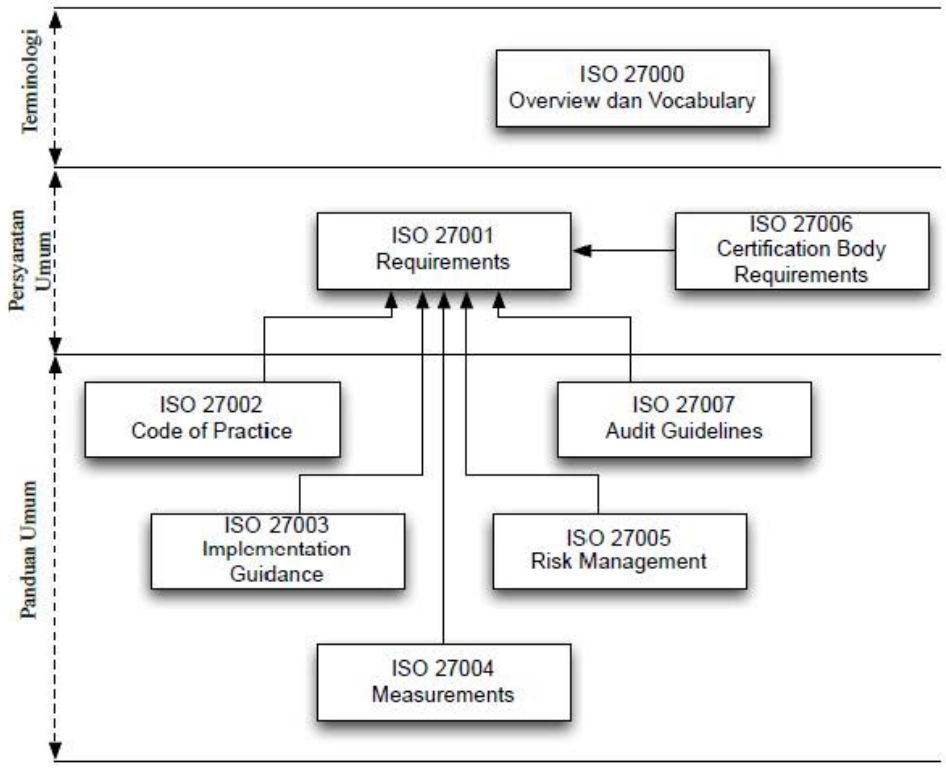
International Organization for Standardization (ISO) adalah sebuah organisasi internasional non-pemerintahan untuk standarisasi. *Internasional Electrotechnical Commission* (IEC) adalah suatu oraganisasi standarisasi internasional yang menyiapkan dan mempublikasikan standar internasional untuk semua teknologi elektrik, elektronika dan teknologi lain yang terkait, yang dikenal dengan elektroteknologi. Standarisasi di gunakan untuk mendukung inovasi dan memberikan solusi untuk tantangan global [5]. Seri ISO/IEC 27000 merupakan pembaharuan dari ISO 17799. ISO/IEC 27001:2005 telah diadopsi Badan Standarisasi Nasional (BSN) sebagai Standar Nasional Indonesia (SNI) untuk SMKI [6].

Seri ISO/IEC 27000 terdiri dari [6]:

- ISO/IEC 27000:2009 - ISMS Overview and Vocabulary
- ISO/IEC 27001:2005 - ISMS Requirements

- ISO/IEC 27002:2005 - Code of Practice for ISMS
- ISO/IEC 27003:2010 - ISMS Implementation Guidance
- ISO/IEC 27004:2009 - ISMS Measurements
- ISO/IEC 27005:2008 - Information Security Risk Management
- ISO/IEC 27006:2007 - ISMS Certification Body Requirements
- ISO/IEC 27007 - Guidelines for ISMS Auditing

ISO/IEC 27000 berisi prinsip-prinsip dasar ISMS, definisi sejumlah istilah penting dan hubungan antar standar dalam keluarga ISMS [6]. Standar ini dapat digunakan untuk semua jenis organisasi baik organisasi pemerintahan, komersial, maupun non-komersial. Berikut ini adalah gambar hubungan antar standar dalam ISO/IEC 27000.



Gambar 2. Hubungan Antar Keluarga ISO/IEC 27000 [6]

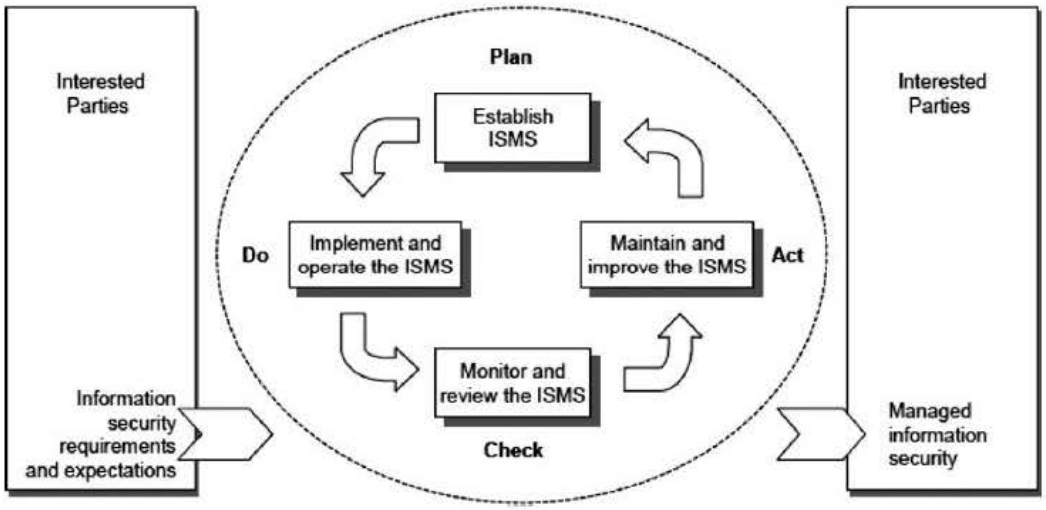
2.5. ISO/IEC 27001

ISO/IEC 27001 dirilis pada tahun 2005. ISO/IEC 27001 ini terus mengalami pembaharuan. Standar ini dibuat sebagai model untuk penetapan, penerapan, pengoperasian, pemantauan, pengkajian, pemeliharaan dan perbaikan ISMS [7]. ISO/IEC 27001 memberikan gambaran umum mengenai kebutuhan yang dibutuhkan

perusahaan/organisasi dalam usahanya untuk mengimplementasikan konsep-konsep keamanan informasi. Penerapan ISO/IEC 27001 disesuaikan dengan tujuan, sasaran dan kebutuhan organisasi. Pendekatan proses ini menekankan pada beberapa hal sebagai berikut [7]:

1) pemahaman persyaratan keamanan informasi organisasi dan kebutuhan terhadap kebijakan serta sasaran keamanan informasi,
2) penerapan dan pengoperasian kontrol untuk mengelola resiko keamanan informasi dalam bentuk konteks resiko bisnis organisasi secara keseluruhan,
3) pemantauan dan tinjau ulang kinerja dan efektivitas ISMS, dan
4) peningkatan berkelanjutan berdasarkan pada pengukuran tingkat ketercapaian sasaran.

Standar ini mengadopsi model "*Plan-Do-Check-Art*" (PDCA), untuk membentuk seluruh proses ISMS. Standar ini memberikan model yang kokoh untuk menerapkan prinsip-prinsip yang ada dalam panduan tersebut yang mengatur asesmen resiko, desain keamanan dan penerapan, manajemen keamanan dan reasesmen [7].



Gambar 3. Model PCDA (ISO 27001)

Berikut ini merupakan penjelasan dari model PCDA:

1) *Plan* (*Establish* ISMS)

   Pada tahapan ini dilakukan dengan menetapkan kebijakan ISMS, sasaran, proses dan prosedur yang relevan untuk mengelola resiko dan meningkatkan keamanan informasi agar memberikan hasil sesuai dengan kebijakan dan sasaran.

2) *Do* (*Maintain and improve the* ISMS)

   Tahapan ini dilakukan dengan menetapkan cara pengoperasian kebijakan ISMS, kontrol, proses dan prosedur-prosedur.

3) *Check* (*Monitor dan review the* ISMS)

   Tahapan ini dilakukan dengan mengkaji dan mengukur kinerja proses terhadap kebijakan, sasaran, praktek-praktek dalam menjalankan ISMS dan melaporkan hasilnya untuk penilaian efektivitasnya.

4) *Act* (*Implement and operate the* ISMS)

   Tahapan ini dilakukan dengan melakukan tindakan perbaikan dan pencegahan berdasarkan hasil evaluasi, audit internal dan tinjauan manajemen tentang ISMS atau kegiatan pemantauan lainya untuk mencapai peningkatan yang berkelanjutan.

Standar ini juga menjelaskan beberapa syarat utama yang harus dipenuhi, antara lain:

- Sistem manajemen keamanan informasi (kerangka kerja proses dan dokumentasi)
- Tanggung jawab manajemen
- Audit internal ISMS
- Peninjauan ulang terhadap manajemen ISMS
- Peningkatan berkelanjutan

Disamping syarat diatas, standar ini juga menberikan persyaratan untuk penetapan sasaran kontrol dan kontrol-kontrol keamanan sistem informasi, yang meliputi 11 area pengamanan, yaitu [6]:

- Kebijakan keamanan informasi
- Organisasi keamanan informasi
- Manajemen aset
- Sumber daya manusia menyangkut keamanan informasi
- Keamanan fisik dan lingkungan
- Komunikasi dan manajemen operasi
- Akses kontrol
- Pengadaan/akuisisi, pengembangan dan pemeliharaan sistem informasi
- Pengelolaan insiden keamanan informasi
- Manajemen kelangsungan usaha (*business continuity management*)
- Kepatuhan

2.6. Manfaat penerapan ISO/IEC 27001

Dengan menerapkan ISO/IEC 27001 akan meningkatkan kepercayaan publik terhadap informasi yang dihasilkan dan diproses oleh sebuah perusahaan serta meningkatkan jaminan kualitas dari sebuah informasi. Standar ini dibuat untuk memudahkan organisasi dalam penerapan ISMS. Standar ini dapat disesuikan kebutuhannya terhadap tujuan, sasaran dan lingkup organisasi. Standar ini juga memungkinkan integrasi dengan model keamanan sistem informasi lainnya.

Meskipun keamanan sistem informasi tidak dapat secara langsung dinilai dengan uang (*intangible*), sebetulnya keamanan sistem informasi dapat diukur dengan besaran uang (*tangible*) [1]. Penerapan ISO/IEC 27001 dapat dijadikan sebagai acuan penilaian keamanan sistem informasi. Penilaian ini biasanya digunakan untuk meyakinkan pihak stakeholder terhadap pentingnya keamanan sistem informasi.

3. KESIMPULAN

Pengelolaan keamanan sistem informasi harus dimulai ketika sebuah sistem informasi dibangun, bukan hanya sebagai pelengkap sebuah sistem informasi. Dengan adanya pengelolaan keamanan sistem informasi yang baik, maka diharapkan perusahaan dapat memprediksi resiko-resiko yang muncul akibat penggunaan sistem informasi sehingga dapat menghindari atau mengurangi resiko yang mungkin dapat merugikan perusahaan.

Seri ISO/IEC 27000 dapat digunakan sebagai standar untuk pengelolaan keamanan sistem informasi. Penggunaan seri ISO/IEC 27000 dapat disesuaikan dengan kebutuhan yang diperlukan perusahaan untuk mencapai sasaran perusahaan terhadap keamanan sistem informasi. ISO/IEC 27001 memberikan gambaran umum mengenai kebutuhan yang dibutuhkan perusahaan/organisasi dalam usahanya untuk mengimplementasikan konsep-konsep keamanan informasi. Dalam hal ini untuk memenuhi standar ISMS perusahaan perlu mengetahui gambaran umum kebutuhan dan cakupan dari ISMS yang tertuang dalam ISO/IEC 27001.

6. DAFTAR PUSTAKA

[1] Rahardjo B, (2002): *Keamanan Sistem Informasi Berbasis Internet*. Bandung.

[2] Harliana P, Perdana A, Prasetyo RMK: *Sniffing dan Spoofing Pada Aspek Keamanan Komputer*. https://www.academia.edu/5088063/Jurnal-Keamanan-Komputer, diakses pada 8 Desember 2015

[3] Syafrizal M: *ISO 17799: Standar Sistem Manajemen Keamanan Informasi*. https://www.academia.edu/5082000/ISO_17799_Standar_Sistem_Manajemen_Keamanan_Informasi, diakses pada 8 Desember 2015

[4] IBISA, (2011): *Keamanan Sistem Informasi*. Andi. Yogyakarta.

[5] www.iso.org

[6] KOMINFO, (2011): *Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik*. Jakarta.

[7] BSN, (2009): *Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2005, IDT)*. BSN. Jakarta.

[8] IT Governance, (2013): *Information Security & ISO 27001*. IT Governance Green Paper. United Kingdom.

[9] ISO/IEC, (2014): *ISO/IEC 27000 Third Edition 2014-01-15*. Switzerland. ISO/IEC.

[10] http://www.republika.co.id/berita/koran/politik-koran/15/02/12/njnap512-keamanan-sistem-informasi-negara-terancam, diakses pada 10 Desember 2015