ISSN : 2503-2844

MODEL PERENCANAAN KEAMANAN SISTEM INFORMASI MENGGUNAKAN PENDEKATAN METODE OCTAVE DAN ISO 27001:2005

Chalifa Chazar[1], Moch. Ali Ramdhani[2]
STMIK Indonesia Mandiri
Jalan Jakarta 79 Bandung
chalifa.chazar@gmail.com[1], mochali@stmik-im.ac.id[2]

Abstrak

Informasi merupakan salah satu aset penting bagi perusahaan yang perlu dijaga kerahasiaannya, integritas, dan ketersediaannya. Semakin tinggi nilai sebuah informasi maka semakin besar pula resiko ancaman yang muncul. Oleh karena itu organisasi membutuhkan suatu standar dalam perencanaan keamanan sistem informasi yang berguna untuk melindungi informasi dari resiko-resiko yang dapat ditimbulkan dari penggunaan Teknologi Informasi (TI) dan Sistem Informasi (SI). Metode OCTAVE merupakan pendekatan sistem terhadap evaluasi resiko keamanan informasi yang komprehensif, sistematik, terarah, dan dapat di lakukan sendiri. Metode OCTAVE dapat digunakan sebagai tahap awal dalam mengklasifikasikan aset-aset penting, resiko, dan penanggulangan resiko. ISO 27001:2005 merupakan standar yang dapat digunakan untuk merancang penyusunan panduan dokumen kebijakan keamanan berupa ruang lingkup dan prosedur untuk pelaksanaan Sistem Manajemen Keamanan Informasi (SMKI). Tujuan penelitian ini adalah untuk memberikan suatu usulan model perencanaan keamanan sistem informasi dengan melakukan penyelarasan terhadap Metode OCTAVE dan ISO 27001:2005. Dengan menggabungkan kedua metode tersebut, diharapkan mampu terbentuk sebuah strategi keamanan informasi yang terarah dan terkendali.

Kata kunci : Keamanan Informasi, SMKI, Metode OCTAVE, ISO 27001.

Abstract

Information is a critical assets for organization that need to be maintanined from the aspects of confidentiality, integrity, and availability. More valuable an information value, the higher the risk of emerging threats. Therefore, an organization need a standard for information security management system that are useful to protect the information from risks of the Information Technology (IT) use and Information System (IS) use. OCTAVE is an approach to information security risk evaluations that is comprehensive, systematic, context drive, and self directed. OCTAVE can be used as a first stage for classification an essential assets, risks, and risk mitigation. ISO 27001:2005 is standard that can be used for designing a document guides for security policy that contains scope and implementation procedure of Information Security Management System (ISMS). The purpose of this research is to provide an ISMS model with combining two methods which is OCTAVE and ISO 27001:2005.With combinig the two methods, is expected to establish an strategy information security that is good directed and controlled.

Keywords : Information Security, ISMS, OCTAVE, ISO 27001.

I. PENDAHULUAN

Penggunaan Teknologi Informasi saat ini telah berkembang menjadi sebuah keharusan untuk mendukung semua kegiatan di organisasi. Informasi merupakan hasil pengolahan data yang diperoleh dari pemrosesan Sistem Informasi (SI) dan Teknologi Informasi (TI). Informasi merupakan salah satu aset yang sangat berharga bagi kelangsungan sebuah organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan yang harus dijaga ketersediaan, ketepatan, dan keutuhannya (Cheristian, Fatoni & Negara). Oleh karena itu kemampuan menyediakan informasi secara cepat dan akurat merupakan hal yang esensial (Chazar, 2015).

Munculnya inovasi-inovasi TI dan SI berguna untuk mendukung besarnya kebutuhan akan informasi. Akan tetapi seiring perkembangannya, TI seringkali dimanfaatkan oleh beberapa pihak yang tidak bertanggungjawab yang dapat menimbulkan ancaman dan resiko yang dapat merugikan perusahaan (Chazar, 2015).

Masalah keamanan sistem informasi sering kali kurang mendapatkan perhatian dari para stakeholder dan pengelola sistem informasi. Terkadang masalah keamanan sering kali diabaikan. Apabila menggangu performansi dari sistem, sering kali keamanan dikurangi atau ditiadakan (Raharjo, 2002, h.1). Pada penerapannya, sering kali keamanan sistem informasi mulai mendapatkan perhatian ketika ancaman sudah terjadi. Resiko kehilangan dan kerusakan informasi merupakan hal yang kritis bagi organisasi, karena informasi merupakan aset penting dalam organisasi yang perlu dijaga keutuhannya. Oleh sebab itu keamanan sistem informasi adalah hal yang perlu direncanakan dengan matang saat perancangan sistem. Mencegah lebih baik daripada mengobati (*prevention is better than cure*).

Setiap organisasi memiliki berbagai informasi yang terkait dengan visi misi, strategi, manajemen, keuangan, pengadaaan, aset, dan informasi-informasi penunjang lainnya. Dimana sebagian besarnya bersifat rahasia. Efektifitas dan efisiensi dari penggunaan TI juga menyebabkan tingkat resiko keamanan sistem informasi yang tinggi. Pentingnya perencanaan Standar Manajemen Keamanan Informasi (SMKI) yang tersusun dengan baik yang dapat menjadi suatu acuan dan dapat diterapkan untuk melindungi informasi dari berbagai macam ancaman kerusakan.

Untuk merancang SMKI yang baik, organisasi perlu mengklasifikasikan aset-aset penting dalam organisasi. Metode OCTAVE merupakan pendekatan sistem terhadap evaluasi resiko keamanan informasi yang komprehensif, sistematik, terarah, dan dapat di lakukan sendiri (Alberts, Dorofee & Allen, 2001, h.1). Metode OCTAVE dapat digunakan sebagai tahap awal dalam mengklasifikasikan aset-aset penting, resiko, dan penanggulangan resiko.

ISO/IEC 27001 merupakan standar yang sering digunakan untuk mengetahui kebutuhan untuk menerapkan keamanan sistem informasi (Chazar, 2015). ISO 27001 dapat digunakan sebagai panduan dalam perencanaan SMKI dimana dalam perencanaanya menyangkut dokumen kebijakan keamanan berserta ruang lingkup dan prosedurnya.

Penelitian ini mencoba menggabungkan kedua kerangka kerja tersebut untuk merancang SMKI, sehingga diharapkan mampu terbentuk sebuah kerangka kerja perencanaan SMKI yang lebih terarah dan terkendali.

II. TINJAUAN PUSTAKA

II.1 Referensi Penelitian

Berikut ini beberapa referensi penelitian yang digunakan sebagai acuan dalam mendukung penelitian ini.

1. Jurnal "*Perencanaan dan Implementasi Standar ISO 27001: 2013 Pada PT. Sinar Sosro Palembang*" (Cheristian, Fatoni & Negara). Penelitian ini membahas mengenai perencanaan standar manajemen keamanan informasi berdasarkan standar ISO 27001.
2. Jurnal "*Manajemen Resiko Keamanan Informasi Dengan Menggunakan Metode Octave (Operationally Critical Threat, Asset, and Vulnerability Evaluation)*" (Supardono, 2009). Penelitian ini membahas mengenai penggunaan metode OCTAVE dalam mengelola resiko keamanan informasi. Pada prakteknya metode OCTAVE lebih menekankan pengelolaan resiko berdasarkan ancaman dan kelemahan terhadap aset-aset informasi organisasi meliputi perangkat keras, perangkat lunak, sistem, informasi dan manusia.

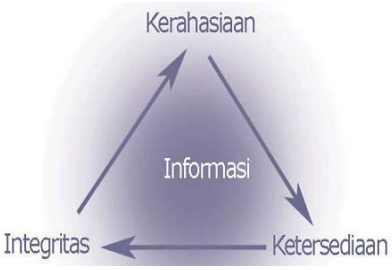
Berdasarkan referensi penelitian diatas, maka penulis mencoba untuk melakukan penelitian untuk menghasilkan sebuah kerangka kerja perencanaan SMKI dengan menggabungkan dua buah metode yaitu metode OCTAVE dan ISO 27001:2005 sebagai sebuah panduan untuk menghasilkan perencanaan SMKI yang lebih detail terhadap resiko ancaman dan kelemahan aset informasi dari suatu organisasi.

II.2 Keamanan Sistem Informasi

Ancaman adalah suatu aksi atau kejadian yang dapat merugikan perusahaan yang mengakibatkan kerugian bisa berupa uang/biaya, tenaga upaya, kemungkinan berbisnis, reputasi nama baik, dan

paling parah dapat membuat organisasi pailit (IBISA, 2011, h.3). Keamanan sistem informasi bertujuan untuk melindungi informasi dan sistem informasi dari berbagai resiko ancaman. Menurut G. J. Simons, keamanan informasi adalah bagaimana kita dapat mencegah penipuan (*cheating*) atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik (Raharjo, 2002, h.2). 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 (Chazar, 2015).

Oleh karena itu keamanan sistem informasi merupakan hal yang perlu diperhatikan sejak awal perencanaan SI. Informasi merupakan salah satu aset penting bagi perusahaan. Keamanan informasi memuat beberapa aspek yang penting, seperti yang terlihat pada gambar 1.



Gambar 1. Aspek Keamanan Sistem Informasi (Syafrizal)

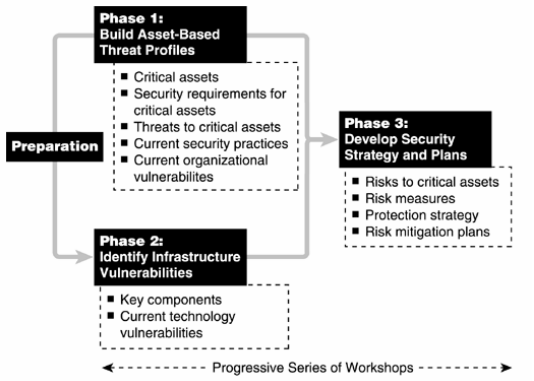
Berikut ini penjelasan dari aspek-aspek keamanan sistem informasi, yaitu (Chazar, 2015):

1. *Confidentiality* (Kerahasiaan)
   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* (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 integritas ini.
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).

II.3 Metode OCTAVE

Metode *Operationally Critical Threat, Aset, and Vulnerability Evaluation* (OCTAVE) merupakan pendekatan sistem terhadap evaluasi resiko keamanan informasi yang komprehensif, sistematik, terarah, dan dapat di lakukan sendiri (Alberts, Dorofee & Allen, 2001, h.1). Metode OCTAVE dapat digunakan untuk mengindentifikasi resiko yang berhubungan dengan aspek-aspek *confidentiality* (kerahasiaan), *integrity* (integritas), dan *availability* (ketersediaan) terhadap aset-aset berharga dan membangun mitigasi bencana untuk mengatasi resiko tersebut.

Metode OCTAVE menggunakan tiga fase pendekatan dalam memeriksa masalah organisasi dan teknologi, memberikan gambaran secara komprehensif tentang kebutuhan keamanan informasi bagi organisasi (Alberts, Dorofee & Allen, 2001, h.3). Tahapan pada metode OCTAVE di gambarkan pada gambar 2 dibawah ini.



Gambar 2. Metode OCTAVE (Alberts, Dorofee & Allen, 2001, h.3)

Berikut ini penjelasan dari fase-fase pada Metode OCTAVE antara lain sebagai berikut.

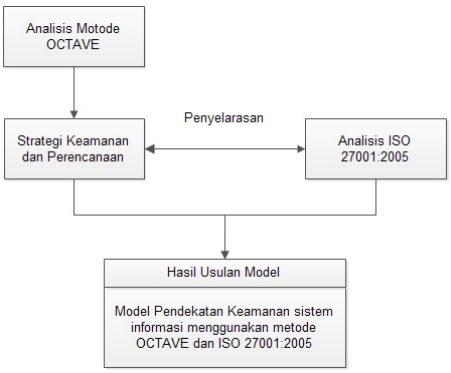
1. *Build Asset-Based Threat Profiles*
   Pada fase ini dilakukan evaluasi dari organisasi.
2. *Indentify Infrastructure Vulnerabilities*
   Pada fase ini dilakukan evaluasi terhadap infrastruktur dari informasi.
3. *Develope Security Strategy and Plans*
   Pada fase akan menghasilkan identifikasi resiko dan merancang mitigasi bencana untuik menangani resiko tersebut.

II.4 ISO 27001:2005

Seri ISO 27001 merupakan bagian seri ISO 27000. ISO 27000, berisi prinsip-prinsip dasar tentang *Information Security Manangement System* (ISMS). ISMS adalah pendekatan sistematis untuk menetapkan, mengimplementasi, operasional, pemantauan, peninjauan, pemeliharaan dan meningkatkan keamanan informasi pada organisasi untuk mencapai tujuan bisnis (Chazar, 2015). ISO 27001 dibuat sebagai model untuk penetapan, penerapan, pengoperasian, pemantauan, pengkajian, pemeliharaan dan perbaikan ISMS (BSN, 2009). ISO 27001 memberikan gambaran umum mengenai kebutuhan untuk mengimplementasikan konsep-konsep keamanan informasi.

III. ANALISIS DAN PERANCANGAN

Tahapan analisis dan perancangan yang dilakukan dalam mengembangkan model perancangan keamanan sistem informasi diilustrasikan pada gambar 3.



Gambar 3. Tahapan Perancangan dan Pengembangan Model

III. 1. Analisis Metode OCTAVE

Proses analisis metode OCTAVE dilakukan sebagai tahapan awal perancangan keamanan sistem informasi untuk mengidentifikasi aset-aset penting, ancaman dan penanganan resiko. Pendekatan ini akan menggunakan fase pertama dan kedua yang terdapat pada metode OCTAVE. Berikut ini analisis dari metode OCTAVE.

1. Fase 1: Membangun Aset Berdasarkan Profile Ancaman
   Fase ini merupakan tahapan untuk melakukan evaluasi dari organisasi. Pada fase ini dilakukan analisis untuk menentukan aset-aset penting dalam organisasi, mengidentifikasi ancaman yang mungkin terjadi, mengidentifikasi hal-hal yang telah dilakukan untuk melindungi aset-aset tersebut, kerentanan organisasi, dan mendefinisikan prasyarat keamanan.
2. Fase 2: Mengidentifikasi Kerentanan Infrastruktur
   Fase ini merupakan tahapan untuk melakukan evaluasi terhadap infrastrukture dari informasi. Pada fase ini dilakukan analisis untuk mengidentifikasi komponen kunci dari infrastruktur informasi dan mengidentifikasi kelemahan dari teknologi yang digunakan.

Hasil analisis dari fase 1 dan fase 2, kemudian akan menjadi masukan bagi proses pengembangan model. Hasil analisis dari fase 1 dan fase 2 pada metode OCTAVE diilustrasikan pada bentuk tabel 1.

Tabel 1. Analisis Metode OCTAVE

Tahapan	No	Hasil
Fase 1	A-1	Aset-aset penting dari organisasi
	A-2	Prasyarat keamanan untuk aset-aset penting
	A-3	Ancaman-ancaman terhadap aset-aset penting organisasi
	A-4	Tindakan dan upaya-upaya keamanan yang sudah dilakukan organisasi
	A-5	Kerentanan dari kebijakan organisasi
Fase 2	B-1	Mengidentifikasi komponen kunci dari infrastuktur informasi
	B-2	Mengidentifikasi kelemahan dari infrastruktur teknologi informasi

III. 2. Analisis ISO 27001:2005

ISO 27001:2005 dapat digunakan untuk merancang penyusunan panduan dokumen kebijakan keamanan berupa ruang lingkup dan prosedur untuk pelaksanaan SMKI. Gambaran struktur dokumentasi berdasarkan ISO 27001:2005 terlihat pada gambar 4.

Gambar 4. Struktur Dokumentasi SMKI (Direktorat Keamanan Informasi, 2011)

Dokumentasi SMKI pada umumnya terdiri dari 3 tingkat, yaitu (Direktorat Keamanan Informasi, 2011):

1. Tingkat 1: Kebijakan dan Standar
   Merupakan dokumen dengan hirarki tertinggi, yang bersifat strategi dalam bentuk kebijakan, standar, sasaran dan rencana terkait pengembangan, penerapan dan peningkatan SMKI.
2. Tingkat 2: Prosedur, Panduan, Petunjuk Pelaksanaan
   Merupakan dokumen yang berisi prosedur dan panduan yang dikembangkan oleh organisasi dan memuat cara menerapkan kebijakan dan penanggung jawab pelaksanaan SMKI.
3. Tingkat 3: Petunjuk Teknis, Instrusi Kerja, Formulir
   Merupakan dokumen yang berisi petunjuk teknis, instruksi kerja dan formulir yang digunakan untuk mendukung pelaksanaan prosedur tertentu sapai ke tingkat teknis.

Hasil analisis dokumen ISO 27001:2005 diilustrasikan pada bentuk tabel 2.

Tabel 2. Analisis Dokumen ISO 27001:2005

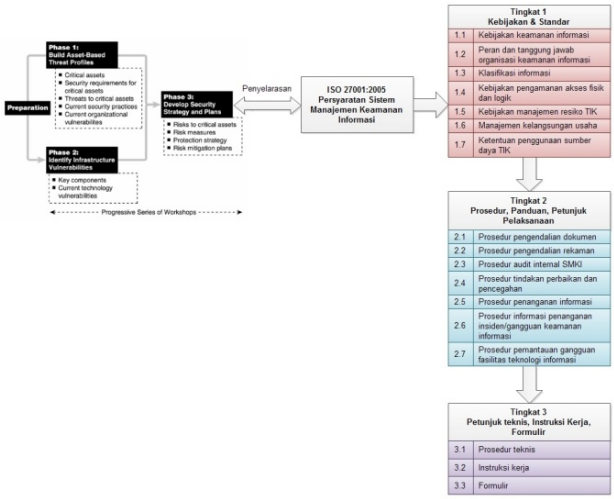
Tingkatan	No	Dokumen
Tingkat 1	1-1	Kebijakan Keamanan Informasi
	1-2	Organisasi, Peran dan Tanggungjawab Keamanan Informasi
	1-3	Panduan Klasifikasi Informasi
	1-4	Kebijakan Manajemen Resiko TIK
	1-5	Kerangka KerjaManajemen KelangsunganUsaha
	1-6	Mengidentifikasi komponen-komponen kunci dari infrastuktur informasi
Tingkat 2	2-1	Pengendalian Dokumen
	2-2	Pengendalian Rekaman
	2-3	Audit Internal
	2-4	Tindakan Perbaikan & Pencegahan
	2-5	Pelabelan, Pengamanan, Pertukaran & *Disposal* Informasi
	2-6	Pengelolaan *Removable* Media & *Disposal* Media
	2-7	Pemantauan Penggunaan Fasilitas TIK
	2-8	*User Access Management*
	2-9	*Teleworking*
	2-10	Pengendalian Instalasi *Software* & Hak Kekayaan Intelektual
	2-11	Pengelolaan Perubahan TIK
	2-12	Pengelolaan & Pelaporan Insiden Keamanan
Tingkat 3	3-1	Prosedur Teknis
	3-2	Instruksi Kerja
	3-3	Formulir

III. 3. Strategi Keamanan dan Perancangan

Berdasarkan hasil analisis yang telah dilakukan terhadap metode OCTAVE pada fase 1 dan fase 2, langkah selanjutnya adalah menentukan perancangan strategi keamanan dan penerapannya. Dimana dalam perancangannya dilakukan kesesuaian dengan dokumen SMKI berdasarkan ISO 27001:2005. Sehingga menghasilkan sebuah dokumen SMKI yang terarah terhadap kebutuhan pengamanan aset-aset penting perusahaan.

III. 4. Hasil Usulan Model

Dari hasil analisis yang dilakukan, maka diperoleh sebuah model usulan perancangan keamanan sistem informasi menggunakan pendekatan metode OCTAVE dan ISO 27001:2005 diilustrasikan pada gambar 5 berikut ini.



Gambar 5. Model Perencanaan Keamanan Sistem Informasi Menggunakan Pendekatan Metode OCTAVE dan ISO 27001:2005

Berikut ini penjelasan langkah-langkah pada model usulan perancangan keamanan sistem informasi menggunakan pendekatan metode OCTAVE dan ISO 27001:2005.

1. Tahap 1: Dilakukan melalui 2 tahapan berdasarkan metode OCTAVE. Pertama melakukan identifikasi aset-aset penting dan identifikasi ancaman terhadap aset-aset. Kedua, melakukan identifikasi terhadap

kelemahan infrastruktur dari teknologi innformasi.
2. Tahap 2: Dilakukan perencanaan keamanan sistem informasi berdasarkan hasil pada tahap 1 dengan penyesuaian berdasarkan dokumen ISO 27001:2005
3. Tahap 3: Berdasarkan hasil pada tahap 2 maka akan didapatkan suatu dokumen perencanaan keamanan sistem informasi berdasarkan 3 level dokumentasi.

Model perencanaan keamanan sistem informasi dengan menggabungkan dua buah metode yaitu Metode OCTAVE sebagai tahapan awal untuk mengidentifikasi resiko berdasarkan ancaman dan kelemahan aset informasi dan Standar ISO 27001:2005 dapat digunakan sebagai acuan kerangka kerja dalam menyusun panduan untuk menghasilkan perencanaan standar manajemen informasi yang lebih detail terhadap resiko ancaman dan kelemahan aset informasi dari suatu perusahaan.

IV. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian yang dilakukan, maka metode OCTAVE dapat digunakan sebagai tools awal untuk mengklasifikasikan aset-aset, resiko dan perancangan mitigasi resiko. Berdasarkan hasil klasifikasi yang dilakukan maka tahapan selanjutnya adalah perencanaan strategi keamanan.

Dimana dalam perancangannya dilakukan kesesuaian dengan dokumen SMKI berdasarkan ISO 27001:2005. Sehingga menghasilkan sebuah dokumen SMKI yang terarah terhadap kebutuhan pengamanan aset-aset penting perusahaan.

Untuk rekomendasi penelitian selanjutnya, usulan model yang dihasilkan dapat secara langsung diimplementasikan pada suatu organisasi sebagai acuan kerangka kerja dalam perencanaan keamanan sistem informasi.

REFERENSI

Chazar, C. (2015). Standar Manajemen Keamanan Sistem Informasi Berbasis ISO/IEC 27001:2005. *Jurnal Informasi, Volume VII No.2/November/2015*, 48-57.

Cheristian, I., Fatoni., Negara, E. S. Perencanaan dan Implementasi Standar ISO 27001:2013 Pada PT. Sinar Sosro Palembang. Diakses 8 Maret 2015 dari http://digilib.binadarma.ac.id/files/disk1/139/123-123- imamcheris-6945-1-jurnali-n.pdf.

Rahardjo, B. (2002). *Keamanan sistem informasi berbasis internet*. Bandung.

IT Governance. (2013). Information Security & ISO 27001. *IT Governanace Green Paper*.

IBISA. (2011). *Keamanan sistem informasi*. Andi: Yogyakarta.

Syafrizal, M. ISO 17799: Standar Sistem Manajemen Keamanan Informasi. Diakses 8 Desember 2015 dari https://www.academia.edu/5082000/ISO_17799_Standar_Sistem_Manajemen_Keamanan_Informasi.

Alberts, C. J., Dorofee, A. J. & Allen, J. H. (2001). *OCTAVE Catalog of Practices* (Version 2.0). Software Engineering Institute: Pittsburgh.

Supardono, B. (2009). Manajemen Resiko Keamanan Informasi Dengan Menggunakan Metode OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation). *Media Elektrika, Vol. 2, No. 1, 2009*, 4-8.

Badan Standarisasi Nasional. (2009). *Information technology - Security techniques - Information security management system - Requirements (ISO/IEC 27001:2005, IDT)*. Jakarta.: BSN.

Direktorat Keamanan Informasi. (2011). *Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik*. Jakarta.: KOMINFO.