Information Security Management System Analysis Menggunakan ISO/IEC 27001 (Studi Kasus: STMIK STIKOM Bali)

Dedy Panji Agustino
Program Studi Sistem Informasi, STMIK STIKOM Bali
Jalan Raya Puputan No.86 Renon Denpasar - Bali, Telp. 0361-244445
e-mail: panji@stikom-bali.ac.id

Abstrak

Informasi merupakan aset paling penting yang dimiliki oleh sebuah organisasi. Di era perkembangan teknologi yang semakin pesat ini, semua informasi yang dimiliki dapat disimpan dan dikelola secara digital. Hal ini membuat proses pengelolaan informasi di dalam organisasi menjadi semakin efektif dan efisien. Di sisi lain, keamanan informasi menjadi suatu hal yang mutlak untuk dipenuhi oleh organisasi. Kebocoran informasi pada sebuah organisasi akan berakibat tidak baik bagi keberlangsungan organisasi tersebut. Keamanan informasi harus memenuhi aspek CIA (Confidentiality, Integrity, dan Availability). Dengan semakin pesatnya perkembangan teknologi, ancaman terhadap aspek C.I.A (Confidentiality, Integrity, dan Availability) dalam sebuah organisasi juga semakin tinggi. Jika salah satu dari aspek C.I.A tersebut tidak dapat dipenuhi oleh organisasi, maka akurasi dan ketersediaan informasi pada organisasi tersebut akan dipertanyakan dan kepercayaan para pengguna informasi tersebut akan menurun sehingga berdampak besar bagi kelangsungan operasional organisasi. STMIK STIKOM Bali merupakan sebuah perguruan tinggi di bidang Teknologi Informasi di Bali yang saat ini sudah memiliki lebih dari 5000 mahasiswa. Hal tersebut membuat kompleksitas pengelolaan informasi yang dimiliki oleh STIKOM Bali cukup tinggi, sehingga aspek keamanan informasi yang dimiliki oleh STIKOM Bali menjadi sangat penting. Namun hingga saat ini belum dilakukan suatu manajemen keamanan informasi yang baik dan terstruktur yang berdasarkan kepada standar keamanan informasi bagi suatu organisasi. Pada penelitian ini, dilakukan proses analisa manajemen keamanan informasi pada infrastruktur teknologi informasi yang ada di STMIK STIKOM Bali, dan didapat hasil pengukuran tingkat kematangan sebesar 1,72 (Initial/Ad Hoc).

Kata kunci: *Informasi, Manajemen Keamanan Informasi.*

Abstract

Information is the most important asset that owned by an organization. In the era of the technology development that increase rapidly, all information can be stored and managed digitally. This makes the information management process within the organization become more effective and efficient. On the other side, information security is an absolute thing to be fulfilled by the organization. Leakage of information on an organization will have an adverse effect on the sustainability of the organization. Information security must include the CIA aspects (Confidentiality, Integrity, and Availability). With the rapid development of technology, threats to aspects of C.I.A (Confidentiality, Integrity, and Availability) in an organization are also getting higher. If one of the aspects of C.I.A cannot be fulfilled by the organization, then the accuracy and availability of information on the organization will be questioned and the trust of the users of that information will decrease so that it has a major impact on the operational continuity of the organization. STMIK STIKOM Bali is a university in the field of Information Technology in Bali which currently has more than 5000 students. This makes STIKOM Bali's information management complexity quite high, so that the information security aspects of STI KOM Bali become very important. But until now there has not been a good and structured information security management based on information security standards for an organization. In this study, an information security management analysis process was carried out on the information technology infrastructure in STMIK STIKOM Bali, and the results is the measurement of the maturity level were 1.72 (Initial / Ad Hoc)

Keywords*: Information, Information Security Management.*

1. Pendahuluan

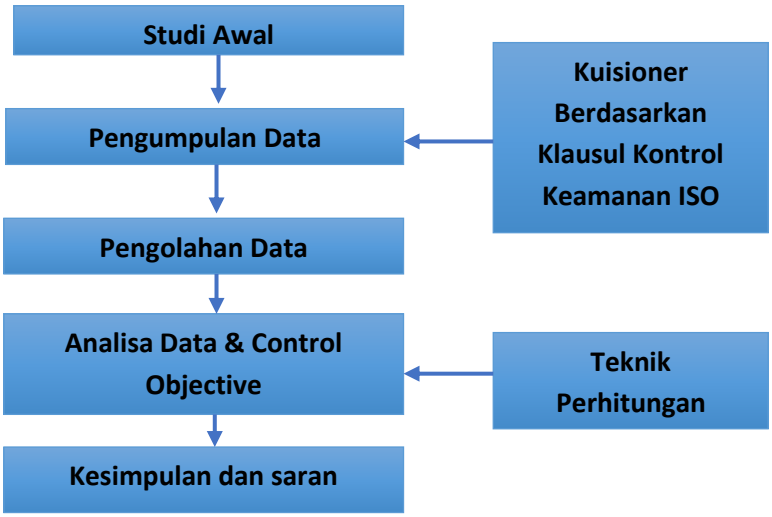
Informasi merupakan sebuah komoditi yang sangat penting bagi sebuah organisasi. Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual. Begitu pentingnya informasi bagi sebuah organisasi menyebabkan aspek keamanan dalam informasi menjadi sangat krusial. Organisasi harus mampu menjamin keamanan informasi yang dimiliki agar informasi tersebut dapat terjaga kerahasiaannya (*confidentiality*), dapat dipastikan keasliannya (*integrity*), serta dapat selalu tersedia ketika dibutuhkan (*availability*).

Dengan semakin pesatnya perkembangan teknologi, ancaman terhadap aspek C.I.A (*Confidentiality*, *Integrity*, dan *Availability*) dalam sebuah organisasi juga semakin tinggi. Jika salah satu dari aspek C.I.A tersebut tidak dapat dipenuhi oleh organisasi, maka akurasi dan ketersediaan informasi pada organisasi tersebut akan dipertanyakan dan kepercayaan para pengguna informasi tersebut akan menurun sehingga berdampak besar bagi kelangsungan operasional organisasi.

STMIK STIKOM Bali merupakan sebuah perguruan tinggi di bidang Teknologi Informasi di Bali yang saat ini sudah memiliki lebih dari 5000 mahasiswa. Hal tersebut membuat kompleksitas pengelolaan informasi yang dimiliki oleh STIKOM Bali cukup tinggi, sehingga aspek keamanan informasi yang dimiliki oleh STIKOM Bali menjadi sangat penting. Namun sejak berdiri pada tahun 2002, belum pernah dilakukan suatu analisa terhadap manajemen keamanan informasi yang bisa diterapkan di STMIK STIKOM Bali, dengan mengacu pada standar atau *framework* tata kelola dan manajemen keamanan informasi yang ada, seperti *framework* COBIT dan ISO/IEC 27001.

2. Metode Penelitian

Metodologi yang digunakan dalam penelitian ini dapat dilihat pada diagram alur penelitian sebagai berikut:



Gambar 1. Alur penelitian.

a. Studi awal
   Dalam melakukan studi awal, penulis melakukan: pencarian materi, pembuatan *draft* kuesioner, serta mempelajari proses TI yang berlangsung di STMIK STIKOM Bali
b. Pengumpulan data
   Pada tahapan pengumpulan data ini, penulis melakukan pengumpulan data yang diperoleh dengan cara pemberian kuesioner kepada pihak – pihak yang terlibat secara langsung dengan proses TI yang berlangsung di STMIK STIKOM Bali, diantaranya pihak *user* dan pihak pengelola sistem dan infrastruktur teknologi informasinya.
c. Pengolahan data
   Pada tahap pengolahan data ini, penulis melakukan pengolahan data dari kuesioner yang di isi oleh para responden dengan cara melakukan pemetaan terhadap klausul kontrol keamanan pada ISO/IEC 27001 dengan hasilnya berupa tingkat kematangan masing-masing proses TI.

Dari kuesioner yang ada, akan dilakukan pembobotan pada jawaban-jawaban dari responden, dengan pembobotan sebagai berikut:

Tabel 1. Pembobotan kuesioner.

Jawaban	Nilai
a	0
b	1
c	2
d	3
e	4
f	5

Kemudian untuk memperoleh nilai tingkat kematangan, digunakan persamaan matematik sebagai berikut:

$$Tingkat\ Kematangan = \frac{Jumlah\ Skor}{Jumlah\ Pertanyaan\ x\ Jumlah\ Responden} \quad (1)$$

d. Analisa data dan *control objective*
Pada tahapan ini, penulis melakukan analisa data dan *control objective* yang diperoleh dari tingkat kematangan, dengan mencari mekanisme *best practice* dalam melakukan pengukuran tingkat kematangan pada proses TI di STMIK STIKOM Bali.

3. Hasil dan Pembahasan

3.1. Pengukuran *Maturity Level*

Jumlah responden yang dipilih dalam pengisian kuesioner di penelitian ini adalah sebanyak 10 orang, yang terdiri dari staf bagian sistem dan jaringan yang memiliki tugas dan tanggung jawab dalam mengelola jaringan komputer di STMIK STIKOM Bali, serta bagian pengembangan sistem informasi yang memiliki tugas dan tanggung jawab dalam pengembangan dan pemeliharaan sistem dan perangkat lunak di STMIK STIKOM Bali. Selain itu responden juga merupakan staf di STMIK STIKOM Bali yang menggunakan aplikasi informasi.

Pengukuran dengan menggunakan ISO 27001 ini fokus pada 4 klausul utama yaitu keamanan sumber daya manusia (A8), keamanan fisik dan lingkungan (A9), pengendalian akses (A11), serta manajemen insiden keamanan informasi (A13). Hasil pengukuran dapat dilihat pada Tabel 2 berikut ini:

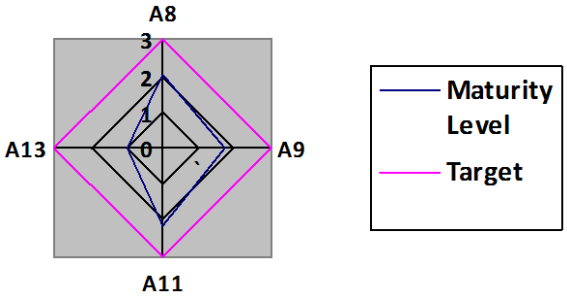
Tabel 2. *Maturity level*.

Proses	Jumlah Skor	Jumlah Pertanyaan	Maturity Level
A8	120	6	2
A9	170	10	1,7
A11	172	8	2,15
A13	30	3	1

Sedangkan untuk target *maturity level* yang ingin dicapai adalah sebagai berikut:

Tabel 3. Target *maturity level*.

Proses	Maturity Level
A8	3,0
A9	3,0
A11	3,0
A13	3,0



Gambar 2. Grafik *maturity level*.

3.2. Analisis Tingkat Kematangan

Dari pengukuran pada 4 klausul yang terdapat dalam ISO 27001 antara lain keamanan sumber daya manusia (A8), keamanan fisik dan lingkungan (A9), pengendalian akses (A11), serta manajemen insiden keamanan informasi (A13), didapat hasil sebagai berikut:

Tabel 4. Tingkat kematangan.

Proses	Maturity Level	Tingkat Kematangan
A8	2	Repeatable but intuitive
A9	1,7	Initial/Ad Hoc
A11	2,15	Repeatable but intuitive
A13	1	Initial/Ad Hoc
Rata - Rata	1,72	Initial/Ad Hoc

Dari Tabel 4 dapat terlihat bahwa dari 4 klausul yang diukur di STMIK STIKOM Bali yaitu keamanan sumber daya manusia (A8), keamanan fisik dan lingkungan (A9), pengendalian akses (A11), serta manajemen insiden keamanan informasi (A13) memiliki tingkat kematangan *Repeatable but intuitive* pada keamanan sumber daya manusia (A8), *Initial/Ad Hoc* pada keamanan fisik dan lingkungan (A9), *Repeatable but intuitive* pada pengendalian akses (A11) dan *Initial/Ad Hoc* pada manajemen insiden keamanan informasi (A13). Secara umum tingkat kematangan yang diperoleh adalah *Initial/Ad Hoc*, sementara target tingkat kematangan yang ingin dicapai adalah pada fase *Defined*.

3.3. Rekomendasi Perbaikan

Dari hasil yang diperoleh, aspek keamanan fisik dan lingkungan, serta aspek manajemen insiden keamanan informasi menjadi prioritas atau fokus utama yang harus dibenahi. Berikut ini beberapa rekomendasi yang dapat digunakan untuk meningkatkan *maturity level* ISO 27001:

Tabel 5. Rekomendasi perbaikan.

Pengendalian	Rekomendasi
Lingkungan keamanan fisik	Tembok terluar sebaiknya terbuat dari konstruksi kuat dan seluruh pintu luar dilindungi dari akses tanpa izin seperti jeruji besi, tanda bahaya dan kunci.
Keamanan kantor, ruang dan fasilitas	Fasilitas penting sebaiknya ditempatkan sedemikian rupa untuk menghindari akses oleh publik. *Intruder system* dipasang sesuai standar profesional dan diuji secara berkala untuk mengamankan seluruh pintu eksternal dan jendela yang mungkin dimasuki. Fasilitas pemrosesan informasi yang dikelola organisasi harus dipisahkan secara fisik dengan fasilitas yang dikelola oleh pihak ketiga. Cadangan peralatan dan media *back-up* sebaiknya ditempatkan dalam jarak yang aman untuk menghindari kerusakan dari kemungkinan kecelakaan di tempat kerja utama.
Sarana Pendukung	Semua peralatan sebaiknya dilindungi dari kegagalan dan ketidaknormalan catu daya listrik atau sarana pendukung lainnya. Terdapat catu daya *multiple feeds* untuk mencegah kegagalan tenaga listrik dari sumber tunggal, UPS dan pembangkit listrik cadangan yang diuji secara berkala. Tombol listrik darurat ditempatkan di dekat pintu darurat di ruang peralatan. Penangkal petir dipasang di semua gedung.
Keamanan kabel dan komunikasi	Saluran listrik dan telekomunikasi ke fasilitas pemrosesan informasi sebaiknya dipasang di bawah tanah atau mendapat perlindungan alternatif yang memadai. Pengkabelan jaringan terlindung dari penyadapan atau kerusakan, seperti menggunakan pipa pengaman atau menghindari *routing* melalui tempat umum
Pemeliharaan Peralatan	Peralatan dipelihara sesuai jadwal servis dan spesifikasi yang direkomendasikan *supplier*. Hanya staf bidang pemeliharaan yang dapat melakukan perbaikan dan servis peralatan.

Layanan insiden keamanan	Sebaiknya disiapkan sebuah pusat layanan kepada pengguna ketika terjadinya sebuah insiden yang mengancam keamanan informasi perusahaan, dan setiap insiden tercatat ke dalam sistem pengelolaan insiden sehingga dapat dijadikan bahan analisa dan evaluasi untuk perbaikan dan pengelolaan keamanan informasi di perusahaan.

4. Simpulan

1. Pada klausul keamanan sumber daya manusia (A8), STMIK STIKOM Bali memiliki tingkat kematangan 2 (*Repeatable but intuitive*).
2. Pada klausul keamanan sumber daya manusia (A8) keamanan fisik dan lingkungan (A9), STMIK STIKOM Bali memiliki tingkat kematangan 1,7 (*Initial/Ad Hoc*)
3. Pada klausul pengendalian akses (A11), STMIK STIKOM Bali memiliki tingkat kematangan 2,15 (*Repeatable but intuitive*).
4. Pada klausul manajemen insiden keamanan informasi (A13), STMIK STIKOM Bali memiliki tingkat kematangan 1 (*Initial/Ad Hoc*).
5. Rata – rata tingkat kematangan yang diperoleh dari 4 klausul ISO 27001 adalah 1,72.

Daftar Pustaka

[1] ISO/IEC, Information Technology - Security Techniques - Information Security Management Systems Requirements, Switzerland: ISO/IEC, 2005.
[2] Badan Standardisasi Nasional, Teknologi Informasi – Teknik Keamanan – Sistem Manajemen Keamanan Informasi - Persyaratan, Indonesia: Badan Standardisasi Nasional, 2009.
[3] Sarno R, Iffano I. Sistem Manajemen Keamanan Informasi. Surabaya: ITSPress, 2009.
[4] Muspa AM, Perancangan Sistem Manajemen Sekuritas Informasi (SMSI) Berdasarkan ISO/IEC 27001. Tesis. Surabaya: Institut Teknologi Sepuluh November, 2010.
[5] The IT Governance Institute, COBIT 4.1: Framework, Control Objectives, Management Guidelines, Maturity Models, IL, USA: IT Governance Institute, 2007.
[6] Weber, Ron. (1999). Information Systems Control and Audit. The University of Virginia: Prentice Hall.
[7] Saull, Ron. (2006). IT Governance A Framework for Performance and Compliance. ITGI Japan Opening Celebration Conference. Tokyo, Japan.