Analisa Manajemen Keamanan Informasi Pada Infrastruktur TI di STMIK STIKOM Bali

Dedy Panji Agustino
STMIK STIKOM Bali
Jalan Raya Puputan No.86 Renon Denpasar - Bali, Telp. +62(361)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.

Kata kunci: *Informasi, Manajemen Keamanan Informasi*.

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 kerahasiannya (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 manajemn 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 2.1 Alur Penelitian

Penelitian dimulai dengan melakukan studi awal, melalui berbagai referensi yang berkaitan dengan topik penelitian, antara lain mengenai sistem manajemen keamanan informasi dan juga tata kelola teknologi informasi. Selanjutnya adalah melakukan identifikasi terhadap *business goals* yang dimiliki oleh STMIK STIKOM Bali. Kemudian setelah mendefinisikan *business goals* selanjutnya adalah memetakan *business goals* dengan IT process, dimana disesuaikan dengan control objective pada framework yang dapat dijadikan acuan sebagai model sistem manajemen keamanan informasi di STMIK STIKOM Bali. Framework manajemen keamanan informasi yang digunakan adalah ISO/IEC 27001, dengan melakukan pemetaan terhadap 11 control objective yang sesuai dengan *business goals* yang ditetapkan.

3. Hasil dan Pembahasan

3.1 Profil STMIK STIKOM Bali

STMIK STIKOM Bali merupakan perguruan tinggi IT yang pertama di Bali. Berdiri sejak tahun 2002, hingga saat ini STMIK STIKOM Bali sudah memiliki lebih dari 5000 mahasiswa yang aktif. Visi dan misi dari STMIK STIKOM Bali adalah :

Visi :

STIKOM Bali mempunyai visi menjadi perguruan tinggi unggulan dan berkualitas di bidang ICT (Informasi Communication Technology) tahun 2020

Misi :

1. Menyelenggarakan Pendidikan Tinggi secara profesional dan berkualitas.
2. Menjalin kerja sama dengan berbagai kalangan baik dalam maupun luar negeri dalam rangka pengembangan dan peningkatanKualitas STIKOM Bali
3. Memberikan manfaat yang sebesar-besarnya untuk kepentingan seluruh lapisan masyarakat khususnya komunitas ICT
4. Mewujudkan Sekolah Tinggi sebagai mitra kerja berbagai pihak yang saling menguntungkan baik dalam maupun luar negeri.
5. Menjadi wadah yang dapat dibanggakan dan memberi rasa aman dan nyaman bagi seluruh civitas akademika

Guna mendukung proses bisnis yang ada di STMIK STIKOM Bali, maka penerapan sistem informasi dan juga infrastruktur teknologi informasi sudah dilakukan. Beberapa sistem informasi yang berjalan di

STMIK STIKOM Bali antara lain sistem informasi akademik, sistem informasi keuangan, sistem informasi inventori aset, hingga sistem informasi online yang digunakan dalam proses belajar mengajar seperti sistem informasi dosen dan juga e-learning.

Dalam menjalankan sistem yang sudah terkomputerisasi, maka tentu saja STMIK STIKOM Bali sudah memiliki perangkat keras (hardware) yang berfungsi sebagai alat untuk menjalankan sistem informasi yang digunakan termasuk Sistem Informasi Akademik (SINAK). Perangkat keras tersebut antara lain komputer server, komputer client, serta perangkat keras jaringan yang menghubungkan seluruh koneksi yang ada di STMIK STIKOM Bali. Daftar perangkat yang mendukung sistem informasi di STMIK STIKOM Bali dapat dilihat pada tabel 3.1 berikut ini :

Tabel 3.1 Daftar Perangkat Pendukung TI di STMIK STIKOM Bali

Kategori Alat : Router					
No	Nama Alat	Jenis Alat	Sistem Operasi	Lokasi Penempatan	Keterangan
1	Distribusi STIKOM	Mikrotik RB 1100AHx2	Mikrotik v6.2	Ruang Server	Untuk Distribusi ke semua server, router, lab STIKOM
2	Juniper SSG 140	NetScreen SSG 140	Screen OS v5.4.0r1a.0	Ruang Server	Untuk Pengaturan IP Lokal Manajemen
3	Catalist 2960	CISCO Catalist 2960	CISCO OS	Ruang Server	Dipergunakan untuk creator vlan
4	AT-8000S	Allied Telesis 8000S/24	AT OS	Ruang Server	Remote via TELNET
5	Blueline Router	Mikrotik RB 450g	Mikrotik OS	Ruang Server	Koneksi ke FO_Access
6	Wireless-Controller	WLC 2500	Cisco OS	Ruang Server	
7	Wifi-&-Lab VLAN	Mikrotik RB450g	Mikrotik OS	Ruang Server	VLAN SmartWifi dan Lab
8	Management VLAN	Mikrotik RB450g	Mikrotik OS	Ruang Server	VLAN Management
9	SmartSwitch LT1	SG200-26P	CISCO IOS	Ruang Server	Koneksi untuk Lantai 1
10	SmartSwitch LT2	SG200-26P	CISCO IOS	Ruang Server	Koneksi untuk Lantai 2
11	SmartSwitch LT3	SG200-26P	CISCO IOS	Ruang Server	Koneksi untuk Lantai 3
12	SmartSwitch LT3	SG200-26P	CISCO IOS	Ruang Server	Koneksi untuk Lantai 3
Kategori Alat : Komputer Server					
1	DNS Server	HP Proliant DL380G5	Debian 7.6.0	Ruang Server	
2	Web Server	HP Proliant DL380G5	CentOS	Ruang Server	
3	Webmail Server	HP ML110G7 – E3 -1220	Ubuntu 12.04	Ruang Server	
4	Information System Server	IBM System x3100, HP ProLiant DL160G8-083, HP	Windows Server 2008	Ruang Server	

		Proliant DL380G6			
Kategori Alat : Komputer Client					
1	Personal Computer Staff dan Kepala Bagian	Assembled Personal Computer	Windows 7	Ruang Staf dan Kepala Bagian	

3.2 Identifikasi Business Goals

Adapun business goals dan sasaran STMIK STIKOM Bali untuk keberlangsungan sistem informasi, serta untuk menjamin keamanan informasinya antara lain :

1. Memiliki kerangka acuan untuk memastikan keberlangsungan layanan sistem informasi di STMIK STIKOM Bali.
2. Memiliki dan menerapkan DRP sebagai penanggulangan terhadap bencana yang mungkin terjadi.
3. Tersedianya server backup dan prosedur manajemen backup yang optimal.
4. Terjaminnya keamanan sistem informasi dari serangan-serangan baik dari arah manapun.
5. Memiliki standar kebijakan, prosedur, dan standar keamanan teknologi informasi.
6. Berlangsungnya proses monitoring, pendeteksian, pelaporan, dan penyelesain terkait insiden yang mengancam keamanan sistem informasi.
7. Memiliki personel yang mengelola dan mengembakan sistem informasi beserta infrastruktur teknologi informasi yang terlatih serta tersertifikasi sesuai dengan kompetensinya.
8. Mengimplementasikan *service desk* sebagai *single point of contact* antara pengguna sistem informasi dengan pengelola sistem.
9. Terjadinya proses *monitoring* dan *maintenance* terhadap insiden yang terjadi pada sistem informasi berdasarkan laporan dari pengguna sistem.
10. Memiliki pengaturan hak akses user yang tepat ke dalam sistem dalam rangka penanganan insiden yang terjadi.
11. Memiliki tingkat prioritas penanganan insiden dan pencatatan histori dari insiden yang terjadi.
12. Menciptakan kondisi lingkungan fisik sekitar perangkat infrastruktur TI yang aman.
13. Memastikan ketersediaan sumber daya agar sistem selalu dapat diakses.

Setelah merumuskan *business goals* dan sasaran dari STMIK STIKOM Bali

3.3 ISO/IEC 27001

Salah satu framework yang dapat digunakan dalam merumuskan sistem manajemen keamanan informasi adalah ISO/IEC 27001. ISO/IEC 27001 adalah standar Keamanan Informasi (information security) yang diterbitkan pada Oktober 2005 oleh ISO (The International Organisation for Standardisation) dan IEC (The International Electrotechniral Commission]. Standar ini menggantikan BS-77992:2002 [ISO 27001, 2005]. ISO/IEC 27001: 2005 mencakup semua jenis organisasi (seperti perusahaan swasta, lembaga pemerintahan, dan lembaga nirlaba). ISO/IEC 27001: 2005 menjelaskan syarat-syarat untuk membuat, menerapkan, melaksanakan, memonitor, menganalisa dan memelihara serta mendokumentasikan Information Security Management System (ISMS) atau disebut juga SMKI dalam konteks resiko bisnis organisasi keseluruhan. Gambar 3.1 menjelaskan kelompok ISO/IEC 27001 yang dijadikan standar SMKI.

<table>
<tr><td colspan="2">27000 Fundamental & Vocabulary</td></tr>
<tr><td rowspan="3">27005
Risk
Management</td><td>27001 : ISMS</td></tr>
<tr><td>27002 : Code of Pratice for ISMS</td></tr>
<tr><td>27004 : Metric & Measurement</td></tr>
<tr><td colspan="2">27006 : Guilines on ISMS Accreditation</td></tr>
<tr><td colspan="2">27007 : Guidelines for ISMS Auditing</td></tr>
</table>

Gambar 3.1 ISO/IEC 27000 *family*

ISO/IEC 27001 mendefinisikan keperluan-keperluan untuk Sistem Manajemen Keamanan Informasi (SMKI). SMKI yang baik akan membantu memberikan perlindungan terhadap gangguan pada aktivitas-aktivitas bisnis dan melindungi proses bisnis yang penting agar terhindar dari resiko kerugian/bencana dan kegagalan serius pada pengamanan Sistem Informasi, implementasi SMKI ini akan memberikan jaminan pemulihan operasi bisnis akibat kerugian yang ditimbulkan dalam masa waktu yang tidak lama.

Ada 11 klausul yang terdapat pada ISO/IEC 27001, antara lain : Security policy (kebijakan keamanan informasi), Organization of information security (Organisasi keamanan informasi), Asset management (Manajemen aset), Human resources security (Keamanan sumber daya manusia), Physical and environmental security (Keamanan fisik dan Lingkungan), Communications and operations management (Manajemen Komunikasi dan Operasi), Access control (Akses kontrol), Information system acquisition, development, and maintenance (Pengadaan/akuisisi, pengembangan dan pemeliharaan sistem informasi), Information security incident management (Manajemen insiden keamanan informasi), Business continuity management (Manajemen kelangsungan usaha), Compliance (Kesesuaian).

3.4 Analisa Control Objective

Dari 11 klausul yang terdapat pada framework ISO/IEC 27001, selanjutnya dilakukan pemetaan dengan berdasarkan kepada business goals dari STMIK STIKOM Bali yang telah ditentukan sebelumnya. Hasil pemetaannya dapat dilihat pada tabel 3.2 berikut ini :

Tabel 3.2 Pemetaan Tujuan dan Sasaran dengan IT Process

No	*Business Goals* dan Sasaran	*IT Procces*
1	Memiliki kerangka acuan untuk memastikan keberlangsungan layanan sistem informasi di STMIK STIKOM Bali	*Access Control (A11) & Physical and Environment Security (A9)*
2	Memiliki dan menerapkan DRP sebagai penanggulangan terhadap bencana yang mungkin terjadi	
3	Tersedianya server backup dan prosedur manajemen backup yang optimal	
4	Terjaminnya keamanan sistem informasi dari serangan-serangan baik dari arah manapun	*Information Security Incident Management (A13)*
5	Memiliki standar kebijakan, prosedur, dan standar keamanan teknologi informasi	
6	Berlangsungnya proses monitoring, pendeteksian, pelaporan, dan penyelesain terkait insiden yang mengancam keamanan sistem informasi	
7	Memiliki personel yang mengelola dan mengembakan sistem informasi beserta infrastruktur teknologi informasi yang terlatih serta tersertifikasi sesuai dengan kompetensinya	*Human Resource Security (A8)*
8	Mengimplementasikan *service desk* sebagai *single point of contact* antara pengguna sistem informasi dengan pengelola sistem	*Communication and operation management (A10)*
9	Terjadinya proses *monitoring* dan *maintenance* terhadap insiden yang terjadi pada sistem informasi berdasarkan laporan dari pengguna sistem	
10	Memiliki pengaturan hak akses user yang tepat ke dalam sistem dalam rangka penanganan insiden yang terjadi	*DS10 Manage problems and incidents*
11	Memiliki tingkat prioritas penanganan insiden dan pencatatan histori dari insiden yang terjadi	
12	Menciptakan kondisi lingkungan fisik sekitar perangkat infrastruktur TI yang aman	*Physical and Environment Security (A9)*
13	Memastikan ketersediaan sumber daya agar sistem selalu dapat diakses	

4. Simpulan

Kesimpulan yang didapat dari hasil penelitian "Analisa Manajemen Keamanan Informasi Pada Infrastruktur TI di STMIK STIKOM Bali" antara lain :

1. Framework ISO/IEC 27001 dapat digunakan dalam menyusun sistem manajemen keamanan informasi di STMIK STIKOM Bali
2. ISO/27001 dapat digunakan untuk mengukur sejauh mana tingkat kematangan dari manajemen keamanan informasi yang telah diterapkan di STMIK STIKOM Bali
3. Terdapat lima klausul pada ISO/IEC 27001 yang sesuai dengan business goals STMIK STIKOM Bali yang dapat dijadikan intstrumen pengukuran dan penerapan sistem manajemen keamanan informasi di STMIK STIKOM Bali

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