PERANCANGAN SISTEM MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN ISO 27001 (STUDI KASUS : IT TELKOM)

Askarudin Tamam Eddy Noveka[1], Niken Dwi Cahyani[2], Yanuar Firdaus A.w.[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

---

Abstrak

Informasi merupakan aset organisasi yang harus dilindungi keamanannya. Keamanan informasi bertujuan untuk menjaga kerahasiaan, keutuhan dan ketersediaan informasi. Sebagai pemenuh kebutuhan akan informasi UPT Sisfo belum mempunyai pedoman yang berhubungan dengan proses pengamanan informasi, serta kurang memahami tentang resiko kehilangan informasi dan bagaimana mengendalikan resiko keamanan informasi.

Dalam tugas akhir ini dilakukan proses perancangan sistem manajemen keamanan informasi (SMKI) sebagai langkah awal organisasi untuk mengamankan informasi. SMKI dapat disusun berdasarkan standar internasional ISO 27001. Tahapan dalam proses perancangan SMKI meliputi penentuan ruang lingkup, analisis resiko dan penentuan obyektif kontrol dan kontrol keamanan. Untuk mempermudah melakukan analisis resiko, dibangun aplikasi yang dapat memfasilitasi tahap analisis resiko. Pembangunan aplikasi analisis resiko menggunakan metode waterfall. Setelah itu akan diukur tingkat kedewasaan SMKI untuk mengetahui sejauh mana tingkat kemampuan UPT Sisfo menerapkan SMKI dan untuk menentukan rekomendasi peningkatan keamanan informasi.

Aplikasi yang dibangun mampu mengakomodasi proses analisis resiko dan memberikan kemudahan bagi pengguna. Berdasarkan hasil perancangan SMKI, aset kritis yang ada di UPT Sisfo yaitu Server I-Gracias, Server DNS, Server web IT Telkom, dan lain lain. Serta didapat 24 obyektif kontrol dan 57 kontrol keamanan yang tersebar dalam 8 klausul. Perolehan nilai maturity level seluruh kontrol berada pada level 3.

Kata Kunci : keamanan informasi, Sistem manajemen keamanan informasi, ISO 27001, analisis resiko, maturity level

---

Abstract

Information is organization's asset that must be protected. Information security goal is to protect confidentiality, integrity and availability of information. As information provider UPT Sisfo does not have any guidelines related to information security, lack understanding about losing information risk and how to manage information security risks.

In this final assignment information security management system is designed as a first step of organization to protect information. ISMS can be built using ISO 27001 International standart. Stages in designing process involve determining scope of ISMS, risk analysis, and determining control objective and security control. Application built using waterfall method to facilitate risk analysis process. After that maturity level of ISMS will measured to determine implementation capability of ISMS at UPT Sisfo and given enhancement recommendations.

Application that have built can accomodate the process of risk analysis and give convenience for users. Based on ISMS design, critical assets in UPT Sisfo are I-Gracias Server, DNS Server, Web server IT Telkom, and others. And obtained 24 Objective controls, 57 security controls that spread in 8 clauses. Maturity level of entire control is at 3rd level.

Keywords : information security, information security management system, ISO 27001, Risk analysis , Maturity level.

---

1. Pendahuluan

1.1 Latar Belakang

Informasi merupakan aset yang sangat bernilai bagi organisasi. Sebagaimana aset organisasi yang lain, maka informasi harus dilindungi. Keamanan informasi bertujuan untuk menjaga aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*). Sistem Manajemen keamanan informasi diperlukan karena ancaman terhadap aspek keamanan informasi semakin lama semakin meningkat[3]. Sistem manajemen keamanan informasi (SMKI) bukan merupakan suatu produk melainkan suatu proses untuk menentukan bagaimana mengelola, memonitor dan memperbaiki informasi agar menjadi aman. Penerapan sistem manajemen keamanan informasi yang baik akan memberikan perlindungan terhadap proses bisnis organisasi agar dapat terhindar dari kemungkinan resiko yang terjadi. ISO 27001 merupakan standar internasional yang dapat digunakan organisasi sebagai pedoman untuk menerapkan sistem manajemen keamanan informasi. ISO 27001 menyediakan model yang lengkap terkait dengan bagaimana membangun, menerapkan, operasional, memonitor, mengkaji ulang, memelihara dan mengembangkan sistem manajemen keamanan informasi[9].

Di IT Telkom terdapat UPT sistem informasi (sisfo) yang memiliki peran untuk pemenuhan kebutuhan akan informasi dengan pengembangan dan pelayanan TI untuk pengolahan data[10]. Namun berdasarkan observasi awal didapat bahwa belum adanya pedoman yang berhubungan dengan proses pengamanan informasi, kurangnya pemahaman tentang resiko kehilangan informasi dan pengendalian terhadap informasi. Oleh karena itu dilakukan proses perancangan sistem manajemen keamanan informasi sebagai langkah awal untuk mengamankan informasi dengan memberikan gambaran tentang resiko yang terjadi, dampak serta pengendalian terhadap resiko keamanan informasi. Tahapan penting dalam proses perancangan sistem manajemen keamanan informasi meliputi tahap penentuan ruang lingkup, tahap analisis resiko dan penentuan obyektif kontrol dan kontrol keamanan. Untuk mempermudah melakukan analisis resiko, akan dibangun perangkat lunak yang dapat memfasilitasi tahap analisis resiko.

Setelah didapat objektif kontrol dan kontrol keamanan, maka objektif kontrol dan kontrol keamanan tersebut akan diukur dan ditentukan tingkat kedewasaannya. Tingkat kedewasaan tersebut akan digunakan untuk mengukur sejauh mana UPT Sisfo mampu menerapkan sistem manajemen keamanan informasi yang telah dirancang. Selain itu dengan adanya nilai tingkat kedewasaan dapat ditentukan rekomendasi untuk meningkatkan keamanan informasi pada UPT Sisfo. Metode pengukuran tingkat kedewasaan yang akan digunakan yaitu *System Security Engineering Capability Maturity Model* (SSE CMM)

1.2 Perumusan Masalah

Masalah yang akan dikaji dalam tugas akhir ini adalah:

1. Bagaimana melakukan analisis resiko terhadap aset informasi sehingga dihasilkan daftar resiko yang mungkin terjadi.
2. Bagaimana membangun perangkat lunak yang dapat mempermudah proses analisis resiko.
3. Bagaimana menentukan objektif kontrol dan kontrol berdasarkan ISO 27001 untuk mengurangi resiko pada aset informasi yang sudah teridentifikasi.
4. Bagaimana mengukur tingkat kedewasaan sistem manajemen keamanan informasi menggunakan SSE-CMM.

1.3 Tujuan

Tujuan yang ingin dicapai dalam tugas akhir ini adalah :

1. Menghasilkan daftar resiko terhadap informasi yang mungkin terjadi di UPT Sistem Informasi berdasarkan hasil analisis resiko.
2. Menghasilkan perangkat lunak yang dapat mempermudah dalam proses analisis resiko.
3. Menganalisis resiko berdasarkan aset yang sudah teridentifikasi untuk kemudian menganalisis objektif kontrol dan kontrol keamanan yang sesuai.
4. Menganalisis nilai tingkat kedewasaan sistem manajemen keamanan informasi menggunakan SSE-CMM untuk kemudian dihasilkan usulan rekomendasi peningkatan program keamanan informasi.

1.4 Batasan Masalah

Adapun batasan masalah pada Tugas akhir ini adalah:

1. Proses perancangan sistem manajemen keamanan informasi berdasarkan kondisi UPT Sistem Informasi IT Telkom pada tahun 2011.
2. Proses analisis resiko berdasarkan aset yang berkaitan dengan akademik, karena Road map UPT Sisfo tahun 2011 fokus pada pengembangan sistem akademik.

1.5 Metodologi Penyelesaian Masalah

Dalam penyusunan tugas akhir ini untuk dapat menyelesaikan masalah maka akan dilakukan metodologi sebagai berikut:

a. Identifikasi Masalah

Tahap ini merupakan tahap awal dalam memulai suatu penelitian. Pada tahap ini, penulis melakukan identifikasi terhadap masalah yang akan dibahas. Permasalahan yang akan diangkat dalam penelitian ini adalah keadaan keamanan informasi yang ada di UPT sistem Informasi, serta

bagaimana merancang sebuah sistem keamanan manajemen informasi yang dapat mengurangi resiko terhadap keamanan informasi.

b. Studi Literatur

Studi literatur dilakukan dengan cara mempelajari literatur-literatur baik yang berupa buku (*textbook*), jurnal, dan artikel ilmiah, maupun website yang berhubungan dengan ISO 27001, keamanan informasi, dan proses audit.

c. Pengumpulan data

Dalam tahap ini akan dilakukan pengkajian terhadap resiko keamanan informasi serta ISO 27001 sehingga dihasilkan variabel – variabel apa saja yang dapat digunakan sebagai perancangan keamanan informasi. Serta mencari dan mengumpulkan data yang dapat digunakan untuk proses perancangan terhadap SMKI.

d. Perancangan sistem

Dalam membangun sistem akan digunakan model perancangan *waterfall*.Pertama akan dilakukan analisa kebutuhan sistem, setelah itu akan dilakukan perancangan aplikasi dengan bantual *tools* visio. Kemudian rancangan tersebut akan diimplementasikan ke dalam bahasa yang dikenali computer atau *coding*. Setelah tahapan *coding* akan dilakukan *testing* sebelum akhirnya aplikasi diterapkan.

e. Pengujian dan analisis

Pengujian akan dilakuan terhadap perangkat lunak yang dibangun dan pengujian terhadap hasil perancangan SMKI. Metode pengujian terhadap aplikasi yang digunakan yaitu *black box testing*, dimana focus pengujian terhadap perangkat lunak pada fungsionalitas dan spesifikasi perangkat lunak. Dalam proses analisis akan dilakukan analisa resiko yang terdiri dari identifikasi aset sampai penentuan kontrol keamanan. Dari hasil analisis resiko akan diketahui kemungkinan resiko keamanan informasi yang terjadi di UPT Sisfo.

f. Penyusunan Laporan

Pada tahapan ini dilakukan penyusunan laporan mengikuti kaidah penulisan yang benar dan sesuai dengan ketentun dan sistematika yang ditentukan oleh institusi.

5. Penutup

5.1 Kesimpulan

1. Aplikasi mampu melakukan proses analisa resiko dan memberikan kemudahan kepada pengguna untuk melakukan analisa resiko. Hal ini dilihat dari nilai kemudahan yang diperoleh yaitu 3.67 dari skala 5.
2. Dari hasil analisis resiko dapat disimpulkan bahwa aset kritis di UPT Sisfo yaitu DHCP Server, Authentication server, database server dan web PMB, Server I-Gracias, Server DNS, Backup aplikasi web I-Gracias, Server web IT Telkom, dan Load Balancer.
3. Berdasarkan hasil analisis resiko ditentukan 24 obyektif kontrol dan 57 kontrol keamanan yang tersebar dalam 8 klausul ISO 27001.
4. Hasil maturity level pada seluruh kontrol keamanan yang diukur berada pada level 3, yang berarti kontrol keamanan didefinisikan dengan baik.

5.2 Saran

1. Perlu adanya implementasi sistem manajemen keamanan informasi pada UPT Sisfo yang mengatur keamanan informasi, sehingga didapat kondisi aman yang mendukung visi dan misi organisasi.
2. Dalam tahap analisis resiko dapat dilengkapi dengan melakukan analisis kuantitatif.

Daftar Pustaka

[1] Carnegie Mellon University.2003. Systems Security Engineering Capability Maturity Model Version 3.0. USA

[2] Ermana, Fine.2011. Audit Keamanan Sistem Informasi Berdasarkan Standar ISO 27001 Pada PT. BPR JATIM

[3] Fauzi, Rokhman.2007. Perancangan dan Implementasi Sistem Manajemen Keamanan Informasi berbasis : Standar ISO/IEC 17799, ISO/IEC 27001, Dan Analisis Resiko Metode Octave-S

[4] Gunawan, Hendro., Suhono, R. Driana. 2006. Studi ISO 17799:2005 Dan Systems Security Engineering Capability Maturiy Model (SSE-CMM) Untuk keamanan aplikasi web. ITB

[5] Kurnia, Aries Fajar.2006. Perencanaan kebijakan keamanan informasi berdasarkan ISMS ISO 27001 studi kasus bank XYZ. Universitas Indonesia.

[6] Modul Responsi Rekayasa Perangkat Lunak.Institut Teknologi Telkom

[7] Peltier, T. R., 2001, Information Security Risk Analysis, Auerbach Publications. (tentang aspke keamanan informasi)

[8] Rekiardi.2003. Penerapan Kebijakan Keamanan TI Untuk Layanan Data Center Di PT X. Universitas Indonesia.

[9] Sarno, Riyanarto., Iffano, Irsyat. Sistem Manajemen Keamanan Informasi. ITSPress:2009.

[10] Setiawan, Erwin Budi. 2009.Perancangan strategis sistem informasi IT Telkom untuk menuju world class university. Bandung : Institut Teknologi Telkom.

[11] SNI ISO/IEC 27001:2009. Teknologi Informasi-Teknik Keamanan- Sistem manajemen keamanan informasi-persyaratan.

[12] Yulianto, Fazmah Arif (2006). Keamanan Sistem - Manajemen Resiko.