PERANCANGAN AUDIT KEAMANAN INFORMASI BERDASARKAN STANDAR ISO 27001:2005 (STUDI KASUS: PT ADIRA DINAMIKA MULTI FINANCE)

Titus Kristanto[1)], Rachman Arief[2)], Nanang Fakhrur Rozi[3)]
Teknik Informatika, I
Jl. Arief Rachman Hakim No. 100 Surabaya
Telp : 085730370856[1)], 085731102722[2)], 085749792048[2)]
E-mail : tintus.chris@gmail.com[1)], ramanarif@gmail.com[2)], nfrozy@gmail.com[3)]

Abstrak

Manajemen keamanan sistem informasi sangatlah penting bagi perusahaan pembiayaan kredit motor yang terdiri dari strategi dan pembagian tanggung jawab dalam menurunkan resiko yang menjadi ancaman terhadap organisasi perusahaan. Karena semua laporan yang berasal dari kantor-kantor cabang seluruh Indonesia akan dikirim ke kantor pusat setiap hari yang memungkinkan resiko hilangnya data dan informasi rahasia perusahaan. Kerangka kerja manajemen keamanan informasi memiliki tahapan proses yaitu dari membuat tahapan persiapan, identifikasi aset, kebijakan dan dokumen pengelolaan keamanan informasi, operasional Teknologi Informasi (TI), jaringan komunikasi, pengamanan informasi. Jika tidak berdasarkan hasil analisis resiko, akan menyebabkan lemahnya strategi dalam antisipasi ancaman gangguan dan serangan terhadap aset. Dalam penyusunan rencana keamanan seharusnya didasari oleh hasil analisis dan mitigasi resiko, agar strategi keamanan yang diusulkan dapat secara efektif menurunkan resiko yang telah diidentifikasi melalui analisis dan mitigasi resiko. Standar yang digunakan yaitu ISO 27001:2005 karena sangat fleksibel tergantung pada kebutuhan organisasi yang dikembangkan dan fokus pada sistem manajemen keamanan informasi. Dari hasil penelitian menunjukkan bahwa kerangka kerja mampu mendeskripsikan secara komprehensif dengan melibatkan partisipasi seluruh penanggungjawab TI dalam mengevaluasi kelemahan dari sisi teknologi dan kebijakkan, mampu memberikan dukungan kelanjutan proses bisnis dalam rangka antisipasi ancaman dan kelemahan yang terus berkembang sampai saat ini.

Kata kunci : *ISO 27001, Audit, Keamanan Informasi, PT Adira Dinamika Multi Finance, Maturity Level*

Abstract

Information systems security management is essential for a company credit motorcycle financing consisting of a strategy and division of responsibilities in reducing the risk of a threat to enterprise organizations. Because all reports originating from branch offices throughout Indonesia will be sent to the central office every day which allows the risk of loss of data and confidential corporate information. Information security management framework has the stages of the process, from making the stages of preparation, asset identification, policy and document information security management, operational Information Technology (IT), communications networks, information security. If it is not based on the results of risk analysis, will lead to lack of strategy in anticipation of the threat of disruption and attack assets. In preparing the security plan should be based on the results of the analysis and mitigation of risk, so that the security of the proposed strategy can effectively decrease the risks that have been identified through the analysis and mitigation of risk. Standards such as ISO 27001:2005 is used because it is very flexible depending on the needs of the organization which developed and focuses on information security management system. The results showed that the framework is able to describe in a comprehensive manner by involving the whole person in charge of IT in evaluating weaknesses in terms of technology and wisdom, able to provide support for the continuation of the business processes in order to anticipate threats and vulnerabilities continue to evolve until today.

Keywords: *ISO 27001, Audit, Information Security, PT Adira Dinamika Multi Finance, Maturity Level*

1. PENDAHULUAN

Perkembangan teknologi informasi yang semakin pesat, resiko keamanan semakin besar pula. Untuk mencapai tujuan bisnis seringkali perusahaan menggunakan Teknologi Informasi dalam mengelola informasi dalam menciptakan layanan yang berkualitas pada proses bisnis. Lemah kendali pada aset informasi memudahkan pihak

yang tidak bertanggungjawab untuk mencuri atau hanya mengganggu jalannya aktivitas terkait pada aset perusahaan. Meningkatnya tingkat ketergantungan pada informasi sejalan dengan resiko yang mungkin akan timbul masalah. Tahapan dalam pembuatan keamanan informasi disusun berdasarkan gangguan yang terjadi, lokasi penyimpanan aset informasi, pemilihan perangkat keamanan yang sesuai dengan perusahaan. Resiko yang biasa timbul yaitu resiko keamanan informasi yang menjadi penting harus tersedia dan digunakan. Informasi merupakan aset yang paling penting untuk dilindungi dan diamankan. Rencana keamanan informasi merupakan susunan strategi yang harus diterapkan untuk mengurangi kelemahan dan menurunkan potensial resiko yang sedang berjalan yaitu dengan proses merendahkan resiko dan melakukan evaluasi dan kontrol. Adira Finance memerlukan keamanan aset, karena aset merupakan bagian yang penting bagi perusahaan kepada masyarakat untuk kelangsungan kredit kendaraan bermotor, khususnya kredit motor. Maka dari itu, Adira Finance memerlukan audit keamanan informasi untuk memastikan sesuai dengan prosedur yang berlaku. Standar yang digunakan yaitu Standar ISO 27001:2005 karena standar tersebut sangat fleksibel yang dikembangkan tergantung dari kebutuhan organisasi, tujuan organisasi, persyaratan keamanan, proses bisnis dan jumlah pegawai dari struktur organisasi serta menyediakan sertifikat Sistem Manajemen Keamanan Informasi (SMKI) yang diakui internasional, disebut dengan *Information Security Management System Certification* (ISMSC) [4]. Klausul yang digunakan dalam audit keamanan informasi, disesuaikan pada kendala yang ditemukan berdasarkan survei dan interview yaitu : Pengelolaan Aset (Klausul 7), Keamanan Sumber Daya Manusia (Klausul 8), Keamanan Fisik dan Lingkungan (Klausul 9), Kontrol Akses (Klausul 11), dan Manajemen Penanganan Insiden Keamanan Informasi (Klausul 13). Dengan adanya audit keamanan informasi, dapat meningkatkan keamanan informasi, prosedur keamanan informasi, serta menurunkan resiko keamanan informasi.

2. LANDASAN TEORI

Keamanan Informasi

Keamanan informasi berkaitan dengan perlinudngan aset yang berharga terhadap kehilangan, pengungkapan penyalahgunaan, atau kerusakan yang mungkin terjadi upaya dalam menjamin kelangsungan bisnis *(business continuity),* meminimalkan resiko bisnis *(reduce business risk)* dan memaksimalkan pengembalian investasi dan peluang [4]. Keamanan informasi mempunyai keempat tujuan yang sangat mendasar adalah:

a) Kerahasiaan *(Confidentialy)*
   Data dan informasi terjamin kerahasiaannya, hanya dapat diakses pihak-pihak yang berwenang, keutuhan serta konsistensi pada sistem data harus tetap terjaga, sehingga upaya orang yang ingin mencuri data dan informasi akan menjadi sia-sia.
b) Ketersediaan *(Availability)*
   Menjamin data tersedia saat dibutuhkan untuk dapat mengakses informasi dan sumber daya yang otorisasi dan menj0061min haknya untuk mengakses informasi.
c) Integritas *(Integrity)*
   Menjamin konsistensi dan menjamin data sesuai dengan aslinya dan tidak dapat diubah tanpa izin pihak yang berwenang.
d) Penggunaan yang Sah *(Legitimate Use)*
   Menjamin kepastian sumber daya tidak dapat digunakan oleh orang yang tidak berhak.

Selain aspek tersebut, terdapat klasifikasi keamanan informasi sebagai berikut:

1) Keamanan Fisik *(Physical Security)*
   Merupakan strategi untuk mengamankan anggota, aset fisik dan tempat kerja dari berbagai ancaman yang terjadi.
2) Keamanan Pribadi *(Personal Security)*
   Merupakan bagian dari keamanan fisik yang melindungi SDM pada organisasi yang memiliki akses terhadap informasi.
3) Keamanan Operasional *(Operation Security)*
   Fokus pada strategi untuk mengamankan kemampuan organisasi untuk bekerja tanpa ada gangguan.
4) Keamanan Komunikasi *(Communication Security)*
   Bertujuan mengamankan media komunikasi, teknologi komunikasi beserta isinya, serta kemampuan untuk memanfaatkan untuk mencapai tujuan organisasi.
5) Keamanan Jaringan *(Network Security)*
   Fokus pada pengamatan peralatan jaringan data organisasi, jaringan beserta isinya, serta kemampuan untuk menggunakan jaringan dalam memenuhi fungsi komunikasi data organisasi.

Audit

Audit identik dengan aktivitas yang sistematik, independen, dan terdokumentasi dengan menemukan bukti *(audit evidence)* dan evaluasi secara obyektif apakah sudah sesuai dengan kriteria audit yang sudah ditetapkan. Tujuan dari audit adalah untuk memberikan gambaran kondisi tertentu yang berlangsung di perusahaan dan pelaporan mengenai pemenuhan terhadap sekumpulan standar yang terdefinisi [3].

Audit Keamanan
Audit keamanan bertujuan untuk evaluasi sistematis dari keamanan informasi dengan cara mengukur beberapa kriteria yang diterapkan oleh perusahaan. Audit menyeluruh mengenai nilai keamanan konfigurasi fisik sistem dan lingkungan, perangkat lunak, proses penanganan informasi, serta praktek pengguna [3].

Audit Sistem Informasi
Audit Sistem Informasi merupakan proses pengumpulan dan evaluasi bukti untuk menentukan apakah informasi dapat melindungi aset atau efektif dalam menggunakan sumber daya secara efektif [3].

ISO 27001:2005
ISO 27001:2005 merupakan standar dokumen Sistem Manajemen Keamanan Informasi (SMKI) yang memberikan gambaran tentang apa yang seharusnya dilakukan dalam usaha implementasi konsep sistem informasi di perusahaan [5]. Kontrol keamanan berdasarkan ISO 27001:2005 terbagi menjadi 11 klausul kontrol keamanan *(security control),* 39 obyektif kontrol *(control objectives)* dan 133 kontrol keamanan [4].

2.6 PT Adira Dinamika Multi Finance
PT Adira Dinamika Multi Finance (Adira Finance) merupakan perusahaan terbesar yang bergerak di bidang pembiayaan berbagai merk otomotif (motor/mobil) di Indonesia sejak tahun 1990. Pada Maret 2004, Adira Finance melakukan penawaran saham dengan pengalihan 75% kepemilikan ke PT Bank Danamon Indonesia Tbk (Bank Danamon) yang merupakan salah satu bank swasta nasional terbesar oleh Temasek Group dari Singapura. Berkat dukungan Bank Danamon, Adira Finance mengembangkan usaha dengan menciptakan keunggulan kompetitif yang dapat menghasilkan nilai yang tinggi bagi konsumen maupun pemegang saham.

3. METODOLOGI PENELITIAN
Berikut ini langkah-langkah pelaksanaan audit keamanan sistem informasi yang meliputi:
1) Mengidentifikasi Proses Bisnis dan IT
2) Menentukan Ruang Lingkup dan Tujuan Audit Sistem Informasi
3) Mengumpulkan Data
4) Melaksanakan Audit Kepatutan
5) Menentukan *maturity level*
6) Menentukan hasil audit keamanan sistem informasi
7) Menyusun laporan hasil audit keamanan sistem informasi

4. IMPLEMENTASI DAN HASIL
4.1 Identifikasi Proses Bisnis dan IT
Dalam perencanaan proses audit, auditor harus memahami proses proses bisnis dan IT perusahaan yang mau diaudit. Pemahaman yang harus dilakukan yaitu mempelajari dokumen-dokumen yang terkait dengan perusahaan seperti profil perusahaan, visi dan misi perusahaan, struktur organisasi perusahaan, proses bisnis dan TI perusahaan. Pihak auditor juga harus tahu apakah sebelumnya perusahaan telah melaksanakan proses audit.

4.2 Penentuan Ruang Lingkup dan Tujuan Audit Sistem Informasi
Ruang lingkup yang dilakukan dengan melakukan observasi, wawancara dan kuesioner. Hasil dari penentuan berupa wawancara dengan pihak PT Adira Dinamika Multi Finance yang dimana masih ada kurangnya keamanan terhadap aset, informasi, akses aplikasi. Penerapan hasil ruang lingkup menggunakan standar ISO 27001:2005 dan klausul-klausul yang digunakan pada standar ISO 27001:2005.

Tabel 1 Pemetaan Klausul ISO 27001:2005

Klausul	Deskripsi
7	Prosedur Pengelolaan Aset
8	Prosedur Keamanan Sumber Daya Manusia (SDM)
9	Prosedur Keamanan Fisik dan Lingkungan
11	Prosedur Kontrol Akses
13	Prosedur Manajemen Penanganan Insiden Keamanan Informasi

4.3 Melaksanakan Audit Kepatutan
Melaksanakan audit kepatutan menghasilkan berupa dokumen wawancara, bukti audit, temuan audit dan nilai kematangan pada kontrol keamanan. Setelah didapatkan semua bukti yang ada, kemudian dianalisis dan dievaluasi pada nilai tingkat kemampuan tiap kontrol keamanan.

4.4 Menentukan *Maturity Level*

Setelah menentukan nilai yang sudah ditetapkan, langkah berikutnya yaitu *maturity level*. Kerangka kerja perhitungan *maturity level* dilakukan secara bertahap. Contoh perhitungan *maturity level* dapat dilihat pada Tabel 2. Untuk contoh hasil *maturity level* dapat dilihat pada Tabel 3. Untuk contoh representasi hasil ke dalam diagram radar, dapat dilihat pada Gambar 1.

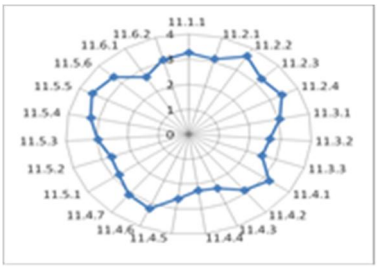
Tabel 2 Contoh Kerangka Kerja Perhitungan *Maturity Level*

11.2	**Manajemen Akses Kontrol**								
No.	**Pernyataan**	**Bobot**	**0**	**1**	**2**	**3**	**4**	**5**	**Nilai**
1	Kebijakan kontrol akses telah dibuat, didokumentasikan dan dikaji ulang berdasarkan kebutuhan bisnis dan keamanan akses	1						√	5
2	Prosedur formal untuk registrasi dan penghapusan user untuk pemberian dan pencabutan akses telah dilakukan ke seluruh sistem informasi dan layanannya	1						√	5
3	Alokasi penggunaan hak akses khusus telah dibatasi dan diatur	1						√	5
4	Alokasi pembuatan dan penggunaan password telah dilakukan melalui proses manajemen yang formal.	1						√	5
5	Manajemen telah melakukan tinjauan ulang terhadap hak akses user secara berkala melalui proses yang formal	1						√	5
Total Bobot		**5**	**Tingkat Kemampuan**						**5**

Tabel 3 Contoh Hasil *Maturity Level* Klausul 11 Kontrol Akses

Klausul	**Obyektif Kontrol**	**Kontrol Keamanan**	**Tingkat Kemampuan**	**Rata-Rata / Obyektif Kontrol**
11 Manajemen Kontrol Akses	11.1 Persyaratan Bisnis Untuk Akses Kontrol	11.1.1 Kebijakan Kontrol Akses	3,25	3,25
	11.2 Manajemen Hak Akses	11.2.1 Registrasi Pengguna	3,12	3,36
		11.2.2 Manajemen hak istimewa atau khusus	3,65	
		11.2.3 Manajemen password user	3,24	
		11.2.4 Tinjauan terhadap hak akses user	3,42	
	11.3 Tanggung Jawab User	11.3.1 Penggunaan password	3,02	2,73
		11.3.2 Peralatan pengguna tanpa penjagaan	2,65	
		11.3.3 Kebijakan *clear desk* dan *clear server*	2,53	
	11.4 Kontrol Akses Jaringan	11.4.1 Kebijakan penggunaan layanan jaringan	3,21	2,80
		11.4.2 Otentiksai pengguna untuk melakukan koneksi keluar	2,87	
		11.4.3 Identifikasi peralatan di dalam jaringan	2,34	
		11.4.4 Perlindungan *remote diagnostic* dan konfigurasi *port*	2,25	
		11.4.5 Pemisahan dalam jaringan	2,59	

Klausul	Obyektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-Rata / Obyektif Kontrol
		11.4.6 Kontrol terhadap koneksi jaringan	3,22	
		11.4.7 Kontrol terhadap *routing* jaringan	3,10	
	11.5 Kontrol Akses Sistem Operasi	11.5.1 Prosedur Log-On yang aman	2,78	3,10
		11.5.2 Identifikasi dan autentikasi user	2,67	
		11.5.3 Sistem manajemen password	2,97	
		11.5.4 Penggunaan utilitas sistem	3,26	
		11.5.5 Sesi *time-out*	3,54	
		11.5.6 Batasan waktu koneksi	3,35	
	11.6 Kontrol Akses Informasi dan Aplikasi	11.6.1 Pembatasan akses informasi	2,67	2,88
		11.6.2 Pengisolasian sistem yang sensitif	3,08	
***Maturity Level* Klausul 11**				**3,02**



Gambar 1 Contoh Representasi Nilai *Maturity Level* Klausul 11 Manajemen Kontrol Akses

4.5 Menentukan Hasil Audit Sistem Informasi

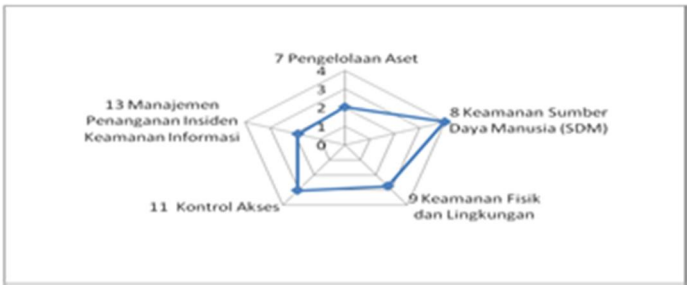
Hasil audit keamanan berupa temuan dan rekomendasi untuk perusahaan, yang berasal dari hasil wawancara, dari sebelumnya evaluasi dan analisis. Laporan hasil audit berupa rekomendasi yang digunakan sebagai saran untuk perbaikan kontrol keamanan. Apabila perhitungan sudah selesai semua, didapatkan nilai dari *maturity level* dari rata-rata semua nilai klausul.

Setelah semua perhitungan selesai, maka didapatkan nilai *maturity level* dari rata-rata nilai keseluruhan klausul, yang dapat dilihat pada Tabel 4.

Tabel 4 Hasil *Maturity Level* Semua Klausul

Klausul	*Maturity Level*
7	2,03
8	3,98
9	2,76
11	3,05
13	1,87
Nilai *Maturity Level*	**2,74**

Didapatkan representasi hasil *maturity level* seluruh klausul pada Gambar 2.



Gambar 2 Representasi Hasil Semua Klausul *Maturity Level*

4.6 Menyusun Laporan Hasil Audit

Setelah melakukan analisis dan evaluasi dari audit pada perusahaan leasing, maka didapatkan beberapa kondisi yang sudah sesuai dengan kontrol ISO 27001:2005 yaitu melakukan pemeriksaan data profil perusahaan, kebijakan, standar, prosedur, melakukan observasi standar prosedur operasi dan hasil wawancara.

Kondisi yang diperbaiki yaitu:
1) Penjadwalan kontrol aset belum dilakukan secara berkala.
2) Tidak ada penanggung jawab khusus dalam perlindungan aset.
3) Tidak ada panduan mekanisme kontrol.
4) Tidak ada pengontrolan dan pencatatan terhadap perubahan.
5) Mengkaji ulang hak akses tidak dilakukan secara berkala.

Beberapa kondisi dari standar ISO 27001:2005 yaitu:
1) Ada aturan tentang tanggung jawab keamanan informasi.
2) Ada parameter pengukuran keamanan.
3) Ada dokumentasi prosedur operasi.
4) Ada dokumentasi terhadap kontrol akses.
5) Ada kebutuhan keamanan sistem baru.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil audit dihasilkan kesimpulan:
1) Perencanaan audit menghasilkan identifikasi ruang lingkup dalam menerapkan manajemen resiko. Langkah audit keamanan informasi dilakukan pembuatan pernyataan, penentuan nilai bobot, dan penentuan nilai kematangan.
2) Pelaksanaan audit didapatkan dari hasil wawancara dalam menentukan dokumen yang diperlukan.
3) Penyalahgunaan *username* dan *password.*
4) Kurang adanya sumber daya manusia yang mengelola.
5) Tidak ada pencatatan mengenai insiden kelemahan keamanan informasi.

5.2 Saran

Beberapa saran yang diberikan yaitu:
1) PT Adira Dinamika Multi Finance dapat melakukan audit dalam runtun rentang waktu 6 bulan sampai 12 bulan agar keamanan informasi tetap terkontrol.
2) Audit keamanan informasi belum menggunakan semua kontrol keamanan, sehingga diharapkan semua sistem PT Adira Dinamika Multi Finance berjalan sesuai dengan proses bisnis yang ada, sesuai dengan Sistem Manajemen Keamanan Informasi (SMKI).
3) Audit keamanan informasi menggunakan ISO 27001:2005 dan penilaian *maturity level* belum memiliki metode penilaian dan diharapkan pengembangan selanjutnya menggunakan yang lain sebagai bahan perbandingan.

6. DAFTAR PUSTAKA

[1] Gondodiyoto, S. 2007. Audit Sistem Informasi Pendekatan COBIT. Jakarta: Mitra Wacana Media.
[2] Herbert J. Mattord, M. W. (2004). Principles of Information Security, Course Technology Ptr.
[3] Sarno, Riyanarto. 2009. Audit Sistem & Teknologi Informasi. Surabaya: ITS Press.
[4] Sarno, R. dan Iffano, I. 2009. Sistem Manajemen Keamanan Informasi. Surabaya: ITS Press.
[5] Badan Standardisasi Nasional Indonesia. *SNI ISO/IEC 27001:2005.*