Analisa *Control Self Assessment Audit* Pada Klausul A.5 *Security Policy* Hingga Klausul A.9 *Physical And Environmental Security* Telkom Flexi Kebon Sirih Jakarta Pusat Menggunakan ISO/IEC 27001

Bramantiyo Eko Putro
Teknik Industri, Universitas Suryakancana
Jl. Pasir Gede Raya, Bojongherang, Cianjur, Kec. Cianjur, Jawa Barat
bramantiyoep91@gmail.com

Abstract

An organization needs some audits for the information security management that have been adapted to prevailing standards for digital information preservation activities that have made the organization's information security management increasingly large and complex enterprise that aims to preserve the importance of the possibility of data loss. These were Kemenkominfo and suggest BUMN such as Telkom Flexi conduct audits of information security management.

In this study will examine how the implementation of information security management audit using ISO / IEC 27001 framework, which is composed of clause A.5 Security Policy, A.6 Organization of Information Security, A.7 Asset Management, A.8 Human Resources Security up to A.9 Physical and Environmental Security. Audit of information security management process begins with searches audit evidence, gap analysis between the standard to the facts found in the field, the value of measurement maturity level of current information security management.

Based on the maturity level of analysis, the conclusions of this study are Telkom Flexi has reached optimal levels at maturity level measurement although still found some of the findings in the field.

Keyword : information security audit, ISO/IEC 27001, gap analysis, maturity level

Abstrak

Suatu organisasi memerlukan adanya mekanisme audit terhadap pengelolaan keamanan informasi yang telah disesuaikan dengan standar yang berlaku karena aktivitas preservasi informasi digital telah membuat semakin besar dan kompleks usaha pengelolaan keamanan informasi yang bertujuan untuk menjaga organisasi dari kemungkinan kehilangan data pentingnya. Hal tersebut disadari Kemenkominfo dan menyarankan BUMN seperti Telkom Flexi melakukan proses audit pengelolaan keamanan informasi.

Pada penelitian ini akan dilakukan kajian bagaimana pelaksanaan audit pengelolaan keamanan informasi dengan menggunakan framework ISO/IEC 27001, yang tersusun dari klausul A.5 Kebijakan Keamanan, A.6 Pengorganisasian Keamanan Infornasi, A.7 Manajemen Aset, A.8 Keamanan Sumber Daya Manusia sampai dengan A.9 Keamanan Fisik dan Lingkungan. Proses audit pengelolaan keamanan informasi dimulai dengan pencarian evidence audit, analisa gap antara standar dengan fakta yang ditemukan di lapangan, pengukuran nilai dari maturity level pengelolaan keamanan informasi saat ini.

Berdasarkan analisis maturity level, kesimpulan dari penelitian ini adalah Telkom Flexi telah mencapai tingkatan Rentang Optimal pada pengukuran maturity level walaupun masih ditemukan beberapa temuan di lapangan.

Kata kunci : audit keamanan informasi, ISO/IEC 27001, gap analysis, maturity level

1. Pendahuluan

Dalam perkembangannya perilaku atau *habits* perusahaan untuk menyimpan data dalam format digital juga mengalami tren peningkatan yang signifikan. Hal ini terlihat dari tingginya angka anggaran dana dan kuota untuk data digital di seluruh dunia. Jurnal internasional *State of Information Global Result 2012* yang diterbitkan oleh Symantec menyebutkan bahwa perusahaan dunia telah menghabiskan US$ 1,1 triliun. Apabila semua data digital perusahaan di dunia dikumpulkan maka akan mencapai angka 2,2 zetabytes atau sebesar 2,2 juta terabytes.

Raymond Goh, Senior Director, System Engineering & Alliances Symantec Asia South Region yang dilansir dalam SWA Magazine juga menerangkan bahwa ada beberapa isu menarik yang harus dihadapi perusahaan-perusahaan di Indonesia dalam menjaga keamanan data digitalnya. Sebesar 65% perusahaan Indonesia meyakini bahwa tantangan terbesar dalam manajemen informasi adalah pertumbuhan data yang sangat cepat. Selain itu 53% perusahaan di Indonesia juga meyakini bahwa masalah yang harus dihadapi adalah kurang mumpuni atau minimnya kemampuan staf IT di perusahaan. Isu yang terakhir adalah mengenai duplikasi data yang diyakini oleh 53% perusahaan.

Kemenkominfo sebagai lembaga yang berwenang mengenai keamanan informasi di Indonesia menyadari bahwa masih banyak instansi pemerintah dan swasta yang belum memiliki atau sedang menyusun kerangka kerja keamanan sistem informasi sesuai standar ISO/IEC 27001. Oleh karena itu, penting juga bagi perusahaan di Indonesia untuk melakukan audit terhadap keamanan

informasi data digitalnya berdasarkan standar yang berlaku. Kemenkominfo yang menerbitkan Panduan Penerapan Tata Kelola Keamanan Informasi menyarankan penggunaan standar ISO/IEC 27001 bagi instansi pemerintah dan swasta khususnya BUMN. Penggunaan ISO/IEC 27001 dipilih karena standar ini sejak 2009 telah diadaptasi menjadi menjadi SNI ISO/IEC 27001:2009 oleh Badan Standardisasi Nasional.

Audit keamanan data digital yang sesuai dengan standar ISO/IEC 27001 juga kurang menjadi perhatian utama bagi Telkom Flexi yang bergerak dalam bisnis informasi dan teknologi. Mulyo Widodo manajer *Risk and Business Continuity* Telkom Flexi penjadwalan audit hanya dilakukan secara insindentil untuk memperbarui masa berlaku standar yang diterapkan Telkom Flexi. Sehingga menunjuk kepada surat nomor C.Tel. 37/PD.520/HCC-G3010000/2012 dilakukan audit keamanan data digital yang bekerja sama dengan pihak eksternal berdasarkan surat pernyataan nomor KD. 69/HK000/Sek-20/2003.

1.1 Rumusan Masalah

Permasalahan yang akan dibahas dalam penelitian ini antara lain :

a. Bagaimana kinerja pengelolaan keamanan informasi pada Telkom Flexi jika dilihat dalam kerangka ISO/IEC 27001?
b. Bagaimana *gap* antara kebijakan, prosedur, sistem, dan persyaratan pengelolaan keamanan informasi Telkom Flexi saat ini dengan praktik terbaik yang didorong oleh standar ISO/IEC 27001?
c. Bagaimana *maturity model* pengelolaan keamanan informasi Telkom Flexi?

1.2 Tujuan Penelitian

Adapun tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut :

a. Menjelaskan kinerja pengelolaan keamanan informasi pada Telkom Flexi dilihat dalam kerangka ISO/IEC 27001.
b. Mengetahui kondisi *gap* antara kebijakan, prosedur, sistem, dan persyaratan pengelolaan keamanan informasi Telkom Flexi saat ini dengan praktik terbaik yang didorong oleh standar ISO/IEC 27001.
c. Mengetahui level *maturity model* pengelolaan keamanan informasi Telkom Flexi.

2. Landasan Teori

2.1 Sistem Informasi

Sistem informasi adalah berbagai kombinasi dari manusia, perangkat keras, perangkat lunak, jaringan komunikasi, sumber data, kebijakan dan prosedur yang mampu menyimpan, mengumpulkan, mengubah, dan menyebarluaskan informasi dalam suatu organisasi. (O'brien and Marakas, 2011:38).

2.2 Tipe Audit

Untuk membatasi ruang lingkup analisa penelitian terhadap infrastruktur dan fasilitas *hardware*, hanya menggunakan salah satu tipe audit yaitu *Control Self Assessment Audit*. Definisi *Control Self Assessment Audit* yang diungkapkan oleh *Pennsylvania Audit, Compliance and Privacy* merupakan penilaian yang difasilitasi untuk mengidentifikasi kesenjangan antara kebijakan saat ini, prosedur, sistem, persyaratan operasi komputer, dan praktik terbaik yang didorong oleh standar industri yang berlaku. Ruang lingkup yang dibahas dalam area kontrol IT adalah strategi IT, manajemen proyek IT, *delivery and support, physical and logical security, disaster recovery and business contingency planning,* dan privasi. (www.upenn.edu, 18 November 2012)

2.3 ISO/IEC 27001

Sebagaimana disebutkan dalam dokumen Panduan Penerapan Tata Kelola KIPPP (Kemenkominfo,2011:10) ISO/IEC 27001:2005 merupakan spesifikasi dan persyaratan yang harus dilengkapi dalam kaitan pembangunan Sistem Manajemen Keamanan Informasi (SMKI). Standar ini memiliki karakter independen terhadap produk teknologi informasi, mengutamakan penggunaan pendekatan manajemen risiko, dibuat untuk melindungi aset dari risiko, dan menambah keyakinan tingkat keamanan bagi pihak yang berkepentingan.

Standar ini dibuat dengan pendekatan proses sebagai model penetapan, penerapan, pengoperasian, pemantauan, tinjau ulang (*review*), pemeliharaan dan peningkatan suatu SMKI. (Kemenkominfo, 2011:10).

ISO/IEC 27001:2005 terdiri atas 133 kendali dalam 11 kategori keamanan informasi (BSNI, 2009:14). Berikut ini adalah pembahasan lebih lanjut mengenai setiap klausul ISO/IEC 27001 :

1. *Information Security Policy*
2. *Organization of Information Security*
3. *Asset Management*
4. *Human Resources Security*
5. *Physical and Environmental Security*
6. *Communication and Operation Management*
7. *Access Control*
8. *Information Systems Acquisiton, Development and Maintenance*
9. *Information Security Incident Management*
10. *Business Continuity Management*
11. *Compliance*

2.4 Maturity Model

Proses penilaian kelengkapan dan kematangan tata kelola keamanan informasi dapat dilakukan melalui dua metode sebagai berikut :

1. Jumlah (kelengkapan) bentuk pengamanan
2. Tingkat kematangan proses pengelolaan pengamanan informasi

Pada penelitian ini digunakan metode kedua untuk menilai kelengkapan dan kematangan tata kelola keamanan informasi. Tingkat kematangan proses pengelolaan keamanan informasi dapat diketahui dengan menggunakan *maturity model.* M*aturity model* digunakan karena merupakan model yang mewujudkan pemikiran dasar manajemen proses sehingga tepat untuk mengukur ISO/IEC 27001 sebagai salah satu standar yang dibuat berdasarkan manajemen proses. (Kemenkominfo,2011:29)

Pengertian *maturity model* merupakan model yang mewujudkan pemikiran dasar mengenai manajemen proses yaitu suatu kualitas sistem atau produk sangat dipengaruhi oleh kualitas dari pengembangan dan pemeliharaan proses yang digunakan. *Maturity model* ini berisi bagian-bagian penting dari proses yang efektif untuk satu atau lebih disiplin dan penggambaran jalur evolusi perkembangan dari tahap *ad hoc*, proses yang belum dewasa untuk didisiplinkan, hingga proses yang telah dewasa dengan peningkatan kualitas dan efektivitas. (*Software Engineering Institute, 2010:5*)

3. Metode Penelitian

3.1 Teknik Pengumpulan Data

Metode pengumpulan data yang digunakan pada penelitian ini :

1. Wawancara terstruktur kepada Manajer *Risk and Business Continuity* dengan menggunakan *list* pertanyaan klausul ISO/IEC 27001.
2. *Nonparticipant-observer* dilakukan dengan pengamatan dokumen-dokumen terkait dan pengamatan keadaan fisik gedung Telkom Flexi Kebon Sirih.
3. Data sekunder diperoleh melalui beberapa literatur yang memiliki kaitan dengan masalah yang sedang dibahas pada penelitian ini, untuk memperoleh informasi yang lebih teoritis yang mempunyai hubungan dengan permasalahan yang diteliti serta memberikan metode alternatif untuk pemecahan masalah yang dihadapi.

3.2 Teknik Audit IT

Audit IT dilakukan sebagai upaya pengumpulan data dan *evidence* yang berkaitan dengan keamanan informasi telkom flexi. Pengumpulan data dan *evidence* mengenai keamanan informasi dilakukan dengan metode wawancara terstruktur dan *nonparticipant-observer*. Struktur pertanyaan dalam proses wawancara diperoleh dari adaptasi klausul ISO/IEC 27001. Setelah proses wawancara dilakukan *nonparticipant-observer* untuk memperoleh *evidence* di lapangan. Hasil proses audit IT akan menjadi bahan analisa dan pembahasan pada bab selanjutnya.

3.3 Teknik Analisis

Teknik analisis yang digunakan pada penelitian ini adalah sebagai berikut :

1. *Gap analysis* akan dilakukan seperti pembahasan pada BAB II untuk mengetahui kondisi kesenjangan keamanan informasi di Telkom Flexi. Berbagai temuan dalam proses audit di Telkom Flexi akan dianalisa dengan membandingkan fakta yang ada di lapangan dengan standar yang berlaku yaitu ISO/IEC 27001. Kondisi yang tampak pada temuan hasil audit akan dibuat analisa dampak dan rekomendasinya agar Telkom Flexi dapat meningkatkan keamanan informasinya sesuai dengan target yang ingin dicapai.
2. Metode *Maturity level* yaitu seperti yang telah dibahas pada BAB II terdapat suatu model yang digunakan untuk untuk menentukan *maturity level* keamanan data digital dari suatu organisasi. Setelah melakukan audit keamanan sistem informasi dan mendapatkan data dan evidence mengenai kondisi keamanan data digital di Telkom Flexi. Hasil audit dan *evidence* akan diberikan nilai sesuai dengan tolak ukur yang ada pada standar ISO/IEC 27001. Nilai keseluruhan klausul yang dilakukan audit akan dirata-rata sehingga menghasilkan suatu nilai *maturity level* yang merefleksikan kondisi keamanan data digital Telkom Flexi.

4. Hasil Dan Pembahasan

4.1 Identifikasi Pengelolaan Keamanan Informasi

Berdasarkan hasil pencatatan yang diperoleh dari observasi dan wawancara yang dilakukan di perusahaan maka diperoleh data sebagai berikut :

1. Pengawasan pelaksanaan kebijakan pengelolaan keamanan informasi di Telkom Flexi Kebon Sirih menjadi tanggung jawab dari bagian *Risk and Business Continuity* yang dikepalai oleh Pak Mulyo Widodo sebagai Manajer *Risk and Business Continuity*. Berdasarkan wawancara dengan kode M/W1/1-9.
2. Telkom Flexi Kebon Sirih tidak lagi menggunakan dokumen dalam bentuk media cetak. Hampir keseluruhan dokumen sudah dilakukan preservasi data ke dalam bentuk digital dan disimpan dalam web portal internal karyawan. Akan tetapi masih ada input data yang berasal dari media cetak seperti penggunaan buku tamu. Berdasarkan wawancara dengan kode M/W1/10-14.
3. Telkom Flexi belum memiliki fasilitas pengamanan fisik berupa dinding gedung yang keseluruhannya tahan terhadap api dan meminimumkan keseluruhan getaran yang mungkin terjadi pada lingkungan fisik akibat bencana yang misalnya seperti gempa bumi. Dalam prosedur pengamanan ruang server P/DTF-CNW/326/01 terlihat hanya ruang server yang memiliki dinding tahan api untuk melindungi *database*. Berdasarkan wawancara dengan kode M/W1/52-66.
4. Telkom Flexi belum sepenuhnya melakukan perawatan dan perlindungan terhadap perkabelan. Masih ditemukan kabel yang belum tertata rapi. Berdasarkan wawancara dengan kode M/W1/67-69.
5. Telkom Flexi mempunyai harapan bahwa kebijakan-kebijakan yang telah mereka susun dapat diterapkan secara menyeluruh dan mendapatkan nilai yang maksimal sesuai standar yang berlaku. Karena banyak *resource* yang digunakan untuk penyusunannya. Berdasarkan wawancara dengan kode M/W1/114-126.

4.2 Gap Analysis

Berdasar pada hasil wawancara dengan bapak Mulyo Widodo dan pengamatan dokumen maupun fisik gedung yang dilakukan di Telkom Flexi, menghasilkan *evidence* dan temuan. Temuan-temuan hasil audit pengelolaan

keamanan informasi Telkom Flexi menunjukkan *gap* antara fakta di lapangan dengan beberapa klausul dari standar ISO/IEC 27001. *Gap analysis* audit pengelolaan keamanan informasi Telkom Flexi adalah sebagai berikut :

Tabel 1 Contoh *WORKING PAPER GAP ANALYSIS*

A.5 Kebijakan Keamanan									
5.1 Kebijakan Keamanan Informasi									
Standar	***Section***	**Pertanyaan Kontrol**	**Jawaban**				***Evidence***	**Temuan**	***Gap***
			Tidak Dilakukan	Dalam Perencanaan	Diterapkan Sebagian	Diterapkan Menyeluruh			
5.1.1	Dokumen Kebijakan Keamanan Informasi	1. Apakah terdapat kebijakan keamanan informasi yang disetujui oleh manajemen, dipublikasikan dan dikomunikasikan dengan tepat ke seluruh karyawan?				✓	Terdapat pada dokumen KD.57/HK-290/ITS-30/2006		Sesuai dengan standar
		2. Apakah kebijakan keamanan menyatakan komitmen manajemen dan menunjukkan pendekatan organisasi dalam mengelola keamanan informasi?				✓	Terdapat pada dokumen KD.57/HK-290/ITS-30/2006		Sesuai dengan standar

4.3 Analisis *Maturity Level*

Pemberian Nilai

Hasil audit pengelolaan keamaan informasi Telkom Flexi Kebon Sirih diberikan nilai menurut kriteria dan standar yang telah ditentukan. Berikut ini adalah tabel analisis penilaian *maturity level* Telkom Flexi Kebon Sirih :

Tabel 2 Contoh *PENILAIAN MATURITY LEVEL*

A.5 Kebijakan Keamanan								
5.1 Kebijakan Keamanan Informasi								
Standar	***Section***	**Pertanyaan Kontrol**	**Jawaban**				**Hasil Pengujian**	**Tingkat Maturity**
			Tidak Dilakukan	Dalam Perencanaan	Diterapkan Sebagian	Diterapkan Menyeluruh		
5.1.1	Dokumen Kebijakan Keamanan Informasi	1. Apakah terdapat kebijakan keamanan informasi yang disetujui oleh manajemen, dipublikasikan dan dikomunikasikan dengan tepat ke seluruh karyawan?				✓	100	
		2. Apakah kebijakan keamanan menyatakan komitmen manajemen dan menunjukkan pendekatan organisasi dalam mengelola keamanan informasi?				✓	100	
		Rata-rata Klausul Kebijakan Keamanan					100	Optimal

Ringkasan Hasil dari Pengujian Keamanan Informasi

Berikut ini adalah penilaian akhir maturity level pada *physical and environmental* Telkom Flexi Kebon Sirih

Tabel 3 PENILAIAN AKHIR *MATURITY LEVEL*

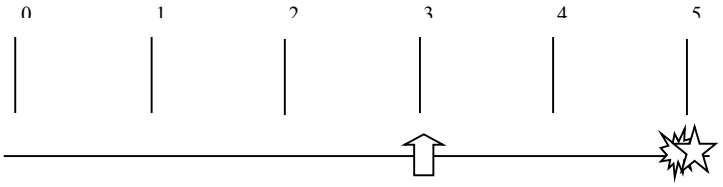
No	Kode	Klausul	Hasil Pengujian	*Maturity Level*
1	A.5	Kebijakan Keamanan	100	Optimal
2	A.6	Pengorganisasian Keamanan Informasi	100	Optimal
3	A.7	Manajemen Aset	100	Optimal
4	A.8	Keamanan SDM	100	Optimal
5	A.9	Keamanan Fisik dan Lingkungan	97	Rentang Optimal
		Rata-rata nilai klausul	**99**	**Rentang Optimal**

Melalui tabel 4.5, dapat dilihat bahwa Telkom Flexi mendapatkan nilai maksimal pada klausul A.5 Kebijakan Keamanan, A.6 Pengorganisasian Keamanan Informasi, A.7 Manajemen Aset, dan A.8 Keamanan SDM. Nilai yang lebih rendah yaitu 97 ditunjukkan pada klausul A.9 Keamanan Fisik dan Lingkungan. Setelah dirata-ratakan *maturity level* akhir Telkom Flexi menunjukkan nilai 99 yang artinya berada pada tingkatan rentang optimal. Artinya pada *level* tersebut Telkom Flexi telah mengimplementasikan proses pengelolaan keamanan informasi secara memuaskan. Hal tersebut dikarenakan perbaikan yang kontinu dan pengukuran tingkat kedewasaan organisasi. Teknologi informasi Telkom Flexi telah diintegrasikan dengan aliran kerja, dan berfungsi sebagai perangkat yang memperbaiki efektifitas dan kualitas. Sehingga Telkom Flexi mampu lebih responsif dalam menghadapi persaingan bisnis.

Analisis *Maturity Level Model*

Berikut ini adalah grafik *maturity level model* Telkom Flexi :

Gambar 1 *Maturity Level* Telkom Flexi



Legenda simbol yang digunakan :

: *maturity level* Telkom Flexi

: standar minimal

: target Telkom Flexi

Legenda untuk peringkat yang digunakan :
0 – Proses manajemen tidak diterapkan sama sekali
1 – Proses bersifat ad hoc dan tidak terorganisir
2 – Memproses mengikuti pola yang teratur
3 – Proses untuk didokumentasikan dan dikomunikasikan
4 – Proses dimonitor dan dan diukur
5 – Praktek terbaik telah dilaksanakan dan terotomatisasi

Setelah dilakukan analisis dengan menggunakan grafik *maturity level model* seperti terlihat pada gambar 4.3 bahwa Telkom Flexi hampir mencapai *level* 5. *Level* 5 adalah level yang menyatakan bahwa praktek terbaik telah dilaksanakan dan terotomatisasi. *Level* yang telah dicapai oleh Telkom Flexi sudah sesuai dengan target *maturity level* yang ingin dicapai perusahaan tersebut. *Maturity level* yang telah dicapai Telkom Flexi juga jauh berada di atas *level* minimum yang harus dicapai perusahaan pada umumnya, yaitu pada *level* 3.

5. Kesimpulan

Berdasarkan penelitian yang telah dilakukan mengenai analisis *control self assesment audit* pada *physical and environmental security* Telkom Flexi Kebon Sirih dengan *framework* ISO/IEC 27001. Maka dapat diambil kesimpulan sebagai berikut :

1. Kinerja pengelolaan keamanan informasi Telkom Flexi Kebon Sirih telah dilaksanakan oleh bagian *Risk and Business Continuity*. Pengelolaan keamanan informasi Telkom Flexi erat kaitannya dengan perlindungan data digital karena proses preservasi data digital yang diterapkan perusahaan. Telkom Flexi Kebon Sirih telah menerapkan pengelolaan keamanan informasi sampai pada klausul *physical and environmental* yang terdapat pada standar ISO/IEC 27001. Telkom Flexi Kebon Sirih memiliki target yang tinggi dalam pencapaian *maturity level* pengelolaan keamanan informasinya.
2. *Gap Analysis* yang dilakukan terhadap pengelolaan keamanan informasi di Telkom Flexi Kebon Sirih ditemukan beberapa temuan yang masih belum sesuai standar ISO/IEC 27001. Temuan tersebut adalah keamanan gedung yang belum sepenuhnya tahan terhadap api dan minim getaran mengakibatkan besarnya resiko bencana seperti kebakaran. Hal tersebut dapat menyebabkan hilangnya informasi perusahaan sehingga aktivitas pengelolaan informasi dan proses bisnis kritis menjadi terganggu. Temuan lain yaitu perkabelan di kantor Telkom Flexi masih belum rapi yang mengakibatkan resiko tinggi terhadap kerusakan akibat pengguna dan kemungkinan lain (binatang). Sehingga memperbesar kemungkinan kehilangan data dan informasi.
3. Penghitungan *maturity level* pada klausul A.9 *Physical and Environmental* ISO/IEC 27001 yang diterapkan Telkom Flexi Kebon Sirih hampir mencapai *level* 5 (Rentang Optimal). Hal ini menunjukkan bahwa Telkom Flexi telah menerapkan sepenuhnya proses pengelolaan keamanan informasi secara memuaskan. Hal tersebut didukung dengan perbaikan yang kontinu dan pengukuran *maturity level* organisasi. Teknologi informasi Telkom Flexi telah diintegrasikan dengan proses bisnis, dan berfungsi untuk memperbaiki efektifitas dan kualitas. Sehingga Telkom Flexi mampu lebih tanggap dalam persaingan bisnis.

6. Saran

Saran-saran yang dapat diberikan berkaitan dengan hasil analisis dan pembahasan dalam penelitian ini adalah :

1. Manajemen Telkom Flexi perlu meningkatkan perlindungan *physical and environmental security* dengan mendesain gedung yang menggunakan tembok tahan api, meminimumkan getaran pada gedung, merapikan dan melindungi seluruh kabel baik yang berkaitan dengan pengolahan informasi atau pun yang tidak.
2. Manajemen Telkom Flexi perlu melaksanakan audit dengan standar yang berlaku yaitu ISO/IEC 27001. Sebaiknya audit dilaksanakan dalam interval yang telah direncanakan. Agar perusahaan selalu mengetahui kondisi perkembangan dari pengelolaan keamanan informasi melalui nilai *maturity level*.
3. Telkom Flexi sebaiknya mampu untuk meningkatkan *maturity level* yang telah dicapai hingga mencapai target maksimal. *Maturity level* aktivitas pengelolaan keamanan informasi yang berada pada tingkatan optimal harus mampu ditingkatkan hingga target pencapaian maksimal sesuai dengan target yang ingin dicapai Telkom Flexi. Upaya tersebut agar dapat menjaga aset informasi perusahaan dengan baik. Sehingga aset informasi dapat digunakan sebagai pertimbangan keputusan manajemen.

7. Daftar Pustaka

[1] Arikunto, Suharsimi, ***Manajemen Penelitian***, Jakarta, Rineka Cipta, 2010.

[2] Babbie, Earl, ***The Practice of Social Research***, Belmont, Wadsworth, 2010.

[3] Badan Standardisasi Nasional. (2009). ***SNI ISO/IEC 27001:2009***. Bogor: BSNI.

[4] CMMI Product Team, ***CMMI® for Acquisition, Version 1.3***. Pittsburgh: Carnegie Mellon Software Engineering Institute, 2010.

[5] Darwas, Rahmadini, 2010, ***Evaluasi Peran Sistem Informasi Manajemen Koperasi Swadharma dengan Menggunakan Model Maturity Level pada Kerangka Kerja COBIT pada Domain Plan and Organise.*** "Thesis S2 pada Gunadarma", Jakarta : tidak diterbitkan.

[6] de Souza, Francis, 2012, ***State of Information Global Results 2012,*** "2012 State of Information Report", 1 (1), 1-12. Retrieved from www.symantec.com.

[7] Fauzi, Rokhman, 2007, ***Perancangan dan Implementasi Sistem Manajemen Keamanan Informasi Berbasis : Standard ISO/IEC 17799, ISO/IEC 27001, dan Analisis Risiko Metode OCTAVE-S,*** "Tugas Akhir S1 pada ITB", Bandung : tidak diterbitkan.

[8] Germain, Rene Saint, 2005, ***Information Security Management Best Practice Based On ISO/IEC 17799,*** The Information Management Journal", 60-66. Retrieved from Arma International Bookstore.

[9] Gladney, H.M, ***Preserving Information Digital,*** New York, Springer, 2010.

[10] Guldentops *et al*, 2002, ***Control and Governance Maturity Survey : Establishing a Reference Benchmark and a Self Assessment Tool,*** "ISACA Journal", 6 (1), 1-8. Retrieved from ISACA Journal Past Issues.

[11] Irmana, Fine, 2011, ***Audit Keamanan Sistem Informasi Berdasarkan Standar ISO 27001 pada PT. BPR JATIM.*** "Tugas Akhir S1", pada STIKOM Surabaya : tidak diterbitkan.

[12] Kahn, M.B, ***Disaster Response and Planning for Libraries, Third Edition,*** Chicago, American Library Asociation, 2012.

[13] Kementrian Komunikasi dan Informatika. (2011). ***Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik***. Jakarta: Kemenkominfo.

[14] Laudon, Kenneth C. and Laudon, Jane P, ***Management Information Systems: Managing The Digital Firm***, Upper Saddle River New Jersey, Pearson Prentice Hall, 2010.

[15] Marina, Ade Putri dan Kridanto, Surendro, 2012, ***Perancangan Model Kapabilitas Proses Pengelolaan Sumber Daya Teknologi Informasi,*** "Jurnal Sarjana Institut Teknologi Bandung Bidang Teknik Elektro dan Informatika", 1 (2), 330-335. Retrieved from stie.itb.ac.id/jurnal.

[16] Maria, Evi and Haryani, Endang, 2011, ***Audit Model Development of Academic Information System: Case Study on Academic Information System of Satya Wacana,*** "Researchers World - Journal of Arts, Science & Commerce", 2 (2), 12-24. Retrieved from Researchers World - Journal of Arts, Science & Commerce archives.

[17] Maria *et al*., 2012, ***The Measurement of Information Technology Performance in Indonesian Higher Education Institutions in The Context of Achieving Institutions Business Goals Using COBIT Framework Version 4.1 (Case Study : SATYA WACANA CHRISTIAN UNIVERSITY, SALATIGA),*** "Researchers World - Journal of Arts, Science & Commerce" 3 (3), 9-19. Retrieved from Researchers World - Journal of Arts, Science & Commerce archives.

[18] Mc Leod, Raymond, ***Sistem Informasi Manajemen, Edisi 10,*** Jakarta, Salemba Empat, 2008.

[19] Moleong, Lexy J., ***Metodologi Penelitian Kualitatif : Edisi Revisi***, Bandung, PT Remaja Rosdakarya, 2012.

[20] Noor, Juliansyah, ***Metodologi Penelitian Skripsi, Tesis, Disertasi, dan Karya Ilmiah,*** Jakarta, Kencana Prenada Media Group, 2011.

[21] Nota Dinas. (2012). C.Tel. 37/PD.520/HCC-G3010000/2012. Jakarta : Telkom Flexi.

[22] OACP, 2009, *Information Technology Audit a Penn : Types of Audit IT* [Online], Tersedia : http://www.upenn.edu/audit/oacp [11 Oktober 2012].

[23] O'brien, James. A. and Marakas, George, ***Management Information System, Tenth Edition,*** New York, Mc Graw Hill, 2011.

[24] Rainer, Kelly and Turban, Efraim, ***Introduction to Information Systems, Second Edition,*** Asia, John Wiley & Sons (Asia) Pte Ltd, 2009.

[25] Rajasa, Raspati Akbar, 2012, ***Audit Keamanan Sistem Informasi Berdasarkan Standar ISO 27001 Menggunakan Information Security Management Maturity Model pada Kementrian Pertanian.*** **"**Tugas Akhir pada IT Telkom Bandung" : tidak diterbitkan.

[26] Rastika, I. (2011, 8 Mei). DPR Juga Bisa Digitalisasi Dokumen. Kompas [Online], Tersedia: http://nasional.kompas.com/read/2011/05/08/13585 82/DPR.Juga.Bisa.Digitalisasi.Dokumen [24 Februari 2012].

[27] Sekaran, Uma and Bougie, Roger, ***Research Methods for Business: A Skill Building Approach,*** West Sussex, John Wiley & Sons Ltd, 2010.

[28] Sugiyono, ***Metode Penelitian Kuantitatif, Kualitatif, dan Kombinasi (Mixed Methods),*** Bandung, Alfabeta, 2011.

[29] Sumber internal perusahahaan. (2012). Profil, Tersedia: http:// www.telkomflexi.com [September 2012].

[30] Surat Pernyataan. (2012). KD. 69/HK000/Sek-20/2003. Jakarta : Telkom Flexi.

[31] Surendro, Kridanto, 2008, ***Rancangan Tata Kelola Teknologi Informasi Uuntuk Pabrik Pupuk,*** "Jurnal Informatika-Petra", 2 (9), 115-121. Retrieved from puslit.petra.ac.id/files/published/journals.

[32] Suryani, Ardayanti Arie, 2009, ***Pengembangan Model Information Technology (IT) Governace pada Organisasi Pendidikan Tinggi Menggunakan COBIT4.1 DOMAIN DS DAN ME,*** "Seminar Nasional Informatika 2009 (semnasIF 2009) UPN Veteran Yogyakarta", 23, 173-182. Retrieved from respository.upnyk.ac.id.

[33] Susanto *et al.*, 2011, ***Information Security Management System Standards: A Comparative Study of the Big Five,*** "International Journal of Electrical & Computer Sciences IJECS-IJENS", 5 (11), 23-29. Retrieved from International Journal of Electrical & Computer Sciences IJECS-IJENS archives.

[34] Telkom Flexi. (2012). ***Proposal Penawaran Telkom Flexi***. Bandung: Telkom Flexi.

[35] Utomo *et al*., 2012, ***Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 pada Kantor Pelayanan Perbendaharaan Surabaya I,*** "Jurnal Teknik ITS", 1 (1), 288-293. Retrieved from ejurnal.its.ac.id.

[36] Widyaningtyas, Tika. (2012, 19 September). Symantec Survei Perangkat Aman untuk Data Perusahaan. SWA [Online], Tersedia: http://swa.co.id/business-research/symantec-survei-perangkat-aman-untuk-data-perusahaan [21 September 2012].

[37] Widyaningtyas, Tika. (2012, 19 September). 65% Perusahaan Indonesia Tertantang Cepatnya Penambahan Data. SWA [Online], Tersedia: http://swa.co.id/business-research/65-perusahaan-indonesia-tertantang-cepatnya-penambahan-data [21 September 2012].

[38] Windari, Shifa. R., 2011, ***Audit Teknologi Informasi Menggunakan COBIT (Control Objective for Information an Related Technology) untuk Mengetahui Kinerja Akuntansi Berbasis Teknologi Informasi pada PT. SALIM IVOMAS PRATAMA, Tbk.*** "Tugas Akhir pada Universitas Gunadarma" : tidak diterbitkan.