ANALISIS MANAJEMEN RISIKO PADA IMPLEMENTASI SISTEM INFORMASI KEAMANAN DI PT.PUPUK SRIWIDJAJA DENGAN *FRAMEWORK* COBIT 4.1

Ivan Harris (ivan.harris96@yahoo.com), **Muara Laut Adong Tarigan(adongtarigan@yahoo.com)**
Suwirno Mawlan (Suwirno@stmik-mdp.net)
Jurusan Sistem Informasi,
STMIK GI MDP

Abstrak : Audit IS/IT yang dilakukan bertujuan untuk mengetahui penerapan tata kelola TI bagian manajemen risiko yang berjalan di PT.Pupuk Sriwidjaja. kemudian memformulasikan serangkaian rekomendasi dari hasil pengamatan pada PT Pupuk Sriwidjaja sehingga mendapatkan hasil akhir berupa dokumentasi untuk mendukung pengembangan sistem lebih lanjut Bentuk Audit IS/IT yang akan dibahas menggunakan *framework* COBIT 4.1, dengan masukan berupa Proses IT yang sedang berjalan saat ini. Kemudian akan diperoleh *Maturity Level*, setelah itu dilakukan analisis terhadap *maturity level* yang sudah didapat. Hasil akhir dari analisis ini berupa rekomendasi, serta metode yang digunakan untuk mencapai rekomendasi yang diusulkan.

Kata kunci : Audit Sistem Informasi, Cobit 4.1 , PT. Pusri Palembang

Abstrack : *audit IS/IT is doing purpose for seeing implementasion IT Governance partion risk management in the PT.Pupuk Sriwidjaja,then formulated recomendation result observation to PT.Pupuk Sriwidjaj until get result that is documentasion for support development system furthermore. Form audit IS/IT in discuss using framework COBIT 4.1, with input process IT in moderate, then will getting maturity level, already that doing analysis to maturty level is getting. Result analysis is recomendation, also method in using for achievement recomendation.*

Key Words : *audit sytem information, Cobit 4.1, PT.Pusri Palembang*

1. PENDAHULUAN

Semakin berkembangnya kemajuan pada dunia Informasi dan teknologi pada abad ini yang berdampak kepada semua aspek di kehidupan manusia. Semua aspek mulai dari pendidikan, bisnis, pemerintahan dan lainnya. Pada awal tahun 90 an penerapan komputerisasi masih menjadi hal yang jarang dikembangkan pada banyak sektor dikarenakan masih mahalnya biaya operasional dan rendahnya manfaat, namun pada era milenium baru penerapan sistem komputerisasi sudah mulai diterapkan pada banyak bidang dan berkembang dengan pesatnya. Berbagai sistem di kembangkan dengan menggunakan media komputer dan pendukungnya dan hal ini membuat sebagian besar sektor mulai mengembangkan sistem informasi pada proses bisnis yang dilaksanakan. Bersama dengan perkembangan sistem informasi saat ini banyak teori-teori ilmiah mengenai pemanfaataan, pengelolaan dan teori teori lainnya.

Salah satu aspek yang menjadi bagian penting dalam sistem informasi dan

pengembangannya adalah aspek keamanan dan manajemen risiko. Seiring dengan berkembangnya sistem informasi pada saat ini beberapa hal penting yang menjadi faktor penentu agar sistem yang berjalan dapat befungsi dengan baik dan benar, karena selain efek positif yang muncul akibat berkembangnya sistem informasi maka permasalahan keamanan dan pengelolaan sumber daya TI juga terjadi. Sebuah institusi atau lembaga yang menggantungkan sebagian besar proses bisnisnya pada sistem informasi akan mengalami kendala yang serius ketika sistem yang diterapkan tidak berjalan dengan semestinya. Pada penelitian kali ini penulis akan melakukan sebuah kajian dan studi ilmiah tentang analisis manajemen risiko pada implementasi sistem informasi keamanan di sebuah perusahaan BUMN di Provinsi Sumatera Selatan yang bergerak pada bidang industri pupuk yaitu PT Pupuk Sriwidjaja (PT PUSRI) dengan menggunakan sebuah metode dari *Information System Auditor and Control Association (*ISACA) yaitu COBIT *FRAMEWORK* 4.1.

2. LANDASAN TEORI

2.1 *Framework COBIT 4.1*

*Contol Objective for Information and Related Technologi (*COBIT*)* memberikan kebijakan yang jelas dan praktik yang baik dalam tata kelola teknologi dengan membantu manajemen senior dalam memahami dan mengelola risiko yang terkait dengan tata kelola teknologi informasi dengan cara memberikan kerangka kerja tata kelola teknologi informasi dan panduan tujuan pengendalian terinci / *detailed contol objective* bagi pihak manajemen, pemilik proses bisnis, pengguna dan juga auditor.
Untuk membuat teknologi informasi berhasil dalam menyampaikan kebutuhan bisnis perusahaan, manajemen harus membuat sistem pengendalian internal atau kerangka kerja. Kerangka kerja COBIT memberikan kontribusi pengendalian kebutuhan ini dengan (ITGI, 2007) ;

- Membuat link dengan kebutuhan bisnis perusahaan
- Mengorganisasikan kegiatan teknologi informasi kedalam suatu proses yang berlaku umum
- Mengidentifikasi sumber daya teknologi informasi utama yang harus dihitung.
- Menentukan tujuan pengendalian manejemen.

Fokus pada COBIT digambarkan oleh model proses yang membagi teknologi informasi menjadi 4 bagian dan 34 proses yang merangkum 210 *detailed control objective* sesuai dengan bidang tanggung jawab, mulai dari perencanaan, membangun, menjalankan dan memonitor implementasi teknologi informasi, dan juga memberikan pandangan *end-to-end* teknologi informasi.

2.2 Sistem Informasi Keamanan

Sistem yang mencegah penipuan (*cheating)* atau, paling tidak, mendeteksi adanya penipuan disebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik.

2.2.1 Ancaman

- Ancaman terhadap keamanan informasi berasal dari individu, organisasi, mekanisme, atau kejadian yang memiliki potensi untuk menyebabkan kerusakan pada sumber – sumber informasi perusahaan.
- Pada kenyataannya, ancaman dapat bersifat internal, yaitu berasal dari dalam perusahaan, maupun eksternal atau berasal dari luar perusahaan. Ancaman dapat juga terjadi secara sengaja atau tidak sengaja.

- Ancaman bersifat internal dari para pegawai tetap, pegawai sementara, konsultan, kontraktor, dan rekan bisnis perusahaan.
- Survey menemukan 49% kejadian yang membahayakan keamanan informasi dilakukan pengguna yang sah dan diperkirakan 81% kejahatan komputer dilakukan oleh pegawai perusahaan.
- Ancaman dari dalam perusahaan mempuyai bahaya yang lebih serius dibandingkan yang dari luar perusahaan, karena kelompok internal memiliki pengetahuan yang lebih mengenai sistem didalam perusahaan.
- Kontrol untuk menghadapi ancaman eksternal baru mulai bekerja jika serangan terhadap keamanan terdeteksi.
- Kontrol untuk menghadapi ancaman internal dibuat untuk memprediksi gangguan keamanan yang mungkin terjadi

3. METODOLOGI

3.1 Studi Pustaka

Studi pustaka dilakukan dengan mengumpulkan beberapa teori, metode ataupun model pada bidang manajemen sistem informasi atau teknologi infromasi pada umumnya, dan juga tata kelola teknologi informasi pada khususnya. Teori, metode maupun model tersebut merupakan metode yang banyak digunakan dan menjadi acuan dalam kegiatan akademis, industri maupun praktisi teknologi informasi pada umumnya.

Adapun sasaran dari studi pustaka itu sendiri adalah :

- Untuk dapat melihat gambaran umum mengenai metode dan kerangka kerja yang digunakan dalam ruang lingkup tata kelola teknologi informasi.
- Membandingkan kerangka kerja yang sudah ada, dengan melakukan identifikasi pola serta mencari kesepadanan dalam kerangka kerja tersebut yang akan dijadikan sebagai alat untuk mengkaji pengelolaan investasi teknologi informasi perusahaan.

3.2 Pengumpulan Data

Dalam penelitian ini data yang dikumpulkan adalah data primer maupun data sekunder.

- Data primer merupakan data yang diambil langsung dari responden yang didapat dari hasil :
  - Kuesioner, pengumpulan data dengan kuesioner ini ditujukan kepada staff TI pada PT. Pupuk Sriwidjaja Palembang dibuat dengan maksud memperoleh target pencapaian dan penilaian dari pencapaian yang sudah dilaksanakan.
  - Wawancara, pengumpulan data dengan cara ini dilakukan dengan tujuan untuk mengetahui proses dan tahapan yang dilakukan sekarang berhubungan dengan pengelolaan sumber daya teknologi informasi, proses pengambilan keputusan, proses pengelolaan investasi teknologi informasi dan juga harapan yang ideal berdasarkan pandangan mereka, sekaligus menentukan faktor – faktor apa saja yang harus diperhatikan pada saat investasi teknologi informasi akan dilakukan.

- Data Sekunder, merupakan data yang diperoleh dari beberapa laporan yang telah dipubliskasikan oleh perusahaan secara internal atau instansi tertentu dan dapat dijaga keabsahannya.

4. HASIL PENGENDALIAN TATA KELOLA *RISK MANAGEMENT*

4.1 Hasil Pengendalian Tata Kelola RM per *Domain* (*primer*)

Hasil evaluasi pengendalian *Risk Management* per *Domain* ini berfungsi untuk mengetahui berapa nilai tingkat kematangan proses pendukung TI primer per *Domain*.

4.1.1 *Plan and Organize* (PO)

Tabel 5.1 Hasil Pengendalian RM *Domain* (PO)

No	Proses	Jumlah Pertanyaan	Jumlah Nilai	Rata-rata
1	PO 4	6	19	3.2
2	PO 6	6	20	3.3
3	PO 9	6	20	3.3
Jumlah proses = 3, jumlah rata – rata = 9.8				
Rata – rata = 3.3				

Dari tabel diatas dapat kita ketahui bahwa nilai Domain PO pada proses pendukung primer adalah 3.3, ini merupakan nilai yang baik bagi sebuah perusahaan dimana sudah ada prosedur dan dilaksanakan

4.1.2 *Delivery and Support* (DS)

Tabel 5.2 Hasil Pengendalian RM per *Domain* (DS)

No	Proses	Jumlah Pertanyaan	Jumlah Nilai	Rata- rata
1	DS 2	6	6	1.0
2	DS 4	6	16	2.7
3	DS 5	6	16	2.7
4	DS 11	6	17	2.8
5	DS 12	6	20	3.3
Jumlah proses = 5, jumlah rata – rata = 12.5				
Rata – rata = 2.5				

Dari tabel diatas dapat kita ketahui bahwa nilai Domain DS pada proses pendukung primer adalah 2.5, ini merupakan nilai yang cukup baik bagi sebuah perusahaan dimana sudah ada prosedur namun belum sepenuhnya dilaksanakan

4.1.3 *Monitoring and Evalution* (ME)

Tabel 5.3 Hasil Pengendalian RM per *Domain* (ME)

No	Proses	Jumlah Pertanyaan	Jumlah Nilai	Rata- rata
1	ME 2	6	24	4.0

2	ME 3	6	23	3.8
3	ME 4	6	22	3.7
Jumlah proses = 3, jumlah rata – rata = 12.0				
Rata – rata = 4.0				

Dari tabel diatas dapat kita ketahui bahwa nilai Domain ME pada proses pendukung primer adalah 4.0, ini merupakan nilai yang ideal sebuah perusahaan dimana sudah ada prosedur, dan sudah dilaksanakan serta adanya pengawasan dari pihak manajemen

4.2 Hasil Pengendalian Tata Kelola RM Per *Domain* (Sekunder)

Hasil evaluasi pengendalian *Risk* nilai tingkat kematangan proses pendukung TI sekunder per Domain.*Management* per *Domain* ini berfungsi untuk mengetahui berapa nilai kematangan per domain

4.2.1 *Plan and Organize* (PO)

Tabel 5.4 Hasil Pengendalian RM *Domain* (PO)

No	Proses	Jumlah Pertanyaan	Jumlah Nilai	Rata-rata
1	PO 1	6	21	3.5
2	PO 2	6	10	1.7
3	PO 3	6	12	2.0
4	PO 7	6	17	2.8
5	PO 8	6	12	2.0
6	PO 10	6	19	3.2
Jumlah proses : 5 , jumlah rata – rata = 15.2				
Rata – rata = 3.0				

Dari tabel diatas dapat kita ketahui bahwa nilai Domain PO pada proses pendukung sekunder adalah 3.0, ini merupakan nilai yang baik bagi sebuah perusahaan dimana sudah ada prosedur dan dilaksanakan

4.2.2 *Acquire and Implement* (AI)

Tabel 5.5 Hasil Pengendalian RM *Domain* (AI)

No	Proses	Jumlah Pertanyaan	Jumlah Nilai	Rata- rata
1	AI 1	6	19	3.2
2	AI 2	6	18	3.0
3	AI 4	6	15	2.5
4	AI 7	6	16	2.7
Jumlah proses = 4 , jumlah rata – rata = 11.4				
Rata – rata = 2.8				

Dari tabel diatas dapat kita ketahui bahwa nilai Domain AI pada proses pendukung sekunder adalah 2.8, ini merupakan nilai yang baik bagi sebuah perusahaan dimana sudah ada prosedur dan dilaksanakan

4.2.3 *Delivery and Support* (DS)

Tabel 5.6 Hasil Pengendalian RM *Domain* (DS)

No	Proses	Jumlah Pertanyaan	Jumlah Nilai	Rata- rata
1	DS 3	6	19	3.2
2	DS 7	6	17	2.8
3	DS 9	6	19	3.2
4	DS 10	6	17	2.8
Jumlah proses = 4, jumlah rata – rata = 12.0				
Rata – rata = 3.0				

Dari tabel diatas dapat kita ketahui bahwa nilai Domain DS pada proses pendukung sekunder adalah 3.0, ini merupakan nilai yang baik bagi sebuah perusahaan dimana sudah ada prosedur dan dilaksanakan

4.2.4 *Monitoring and Evaluation* (ME)

Tabel 5.7 Hasil Pengendalian RM *Domain* (ME)

No	Proses	Jumlah Pertanyaan	Jumlah Jawaban	Rata- rata
1	ME 1	6	20	3.3
Jumlah proses = 1 , jumlah rata – rata = 3.3				
Rata – rata = 3.3				

Dari tabel diatas dapat kita ketahui bahwa nilai Domain ME pada proses pendukung sekunder adalah 3.3, ini merupakan nilai yang baik bagi sebuah perusahaan dimana sudah ada prosedur dan dilaksanakan

5. PEMBAHASAN

Berdasarkan uraian dan pembahasan pada setiap bab sebelumnya, maka dapat ditarik beberapa kesimpulan sebagai berikut :

1. Kondisi manajemen risiko pada implementasi sistem informasi keamanan sudah baik, ini dibuktikan dengan nilai yang diperoleh dari proses pendukung TI secara keseluruhan yaitu 2.8, dimana pada *level* ini sudah ada prosedur dan dilakanakan. Berikut ini adalah nilai *maturiy level* yang didapat dari penelitian penulis :

1.1 Hasil evaluasi pengendalian RM per *domain* (primer)

1.1.1 *Plan and Organize* (PO) mempunyai nilai rata – rata 3.3

1.1.2 *Delivery and Support* (DS) mempunyai nilai rata – rata 2.5

1.1.3 *Monitoring and Evaluation* (ME) mempunyai nilai rata – rata 4.0

1.2 Hasil evaluasi pengendalian RM per *domain* (sekunder)

1.2.1 *Plan and Organize* (PO) mempunyai nilai rata – rata 3.0

1.2.2 *Acquire and Implement* (AI) mempunyai nilai rata – rata 2.8

1.2.3 *Delivery and Support* (DS) mempunyai nilai rata – rata 3.0

1.2.4 *Monitoring and Evaluation* (ME) mempunyai nilai rata – rata 3.3

2. Penerapan audit IS/IT ini harus dilakukan secara berkala, agar terhindar dari kesalahan pengambilan keputusan, kehilangan data, kesalahan operasi komputer dan lain – lain.

6. PENUTUP

[1] Firdaus , Adri Praharja, Tri Hasmoro 2006, Dampak Kematangan TI Organisasi pada Proses *Alignment* Bisnis dengan TI, Jurnal Universitas Indonesia.

[2] Kadir, Abdul 2003, *Pengenalan Sistem Informasi*, Andi, Yogyakarta

[3] Karya, Gede 2004, Pengembangan Model Audit Sistem Informasi Berbasis Kendali, Universitas Katholik Parahyangan, Bandung.

[4] Prof. Jogiyanto & Willly Abdillah, 2011, Sistem Tatakelola Teknologi Informasi, Andi,Yogyakarta

[5] Rahmat M. & Samik-ibrahim 2005, Serba serbi keamanan sistem informasi, Jurnal univerisitas achmad yani, bandung.

[6] Ramadhanty, dwiani 2009, Penerapan Tata Kelola Teknologi Informasi dengan menggunakan COBIT Framework 4.1 : Studi kasus pada PT. Indonesia Power

[7] Riyanarto, Sarno, 2012, Audit Sistem Teknologi Informasi, Informatika, Bandung

[8] Sasongko, Nanang 2009, Pengukuran Kinerja Teknologi Informasi Menggunakan *framework* COBIT versi 4.1 *Ping Test* dan CAAT pada PT.Bank X Tbk, jurnal universitas achmad yani, bandung.

[9] Supriatna, Ade 2010, Analisa Penerapan TOGAF dan COBIT dalam Tatakelola Teknologi Informasi sebagai Usulan kepada Kementrian Energi dan Sumber daya mineral, Jurnal STMIK Subang, Yogyakarta.

[10] Surendro , Krisdanto 2009 Implementasi Tata Kelola Teknologi Informasi, Informatika, Bandung.

[11] Sutedi, Adrian 2012 *Good Corporate Governance*, Sinar Grafika, Jakarta

[12] Wardhani, Dwi Rizki Kesuma 2012, Evaluasi *IT Governance*

berdasarkan COBIT 4.1 (Studi kasus di PT. TIMAH(PERSERO) Tbk), Jurnal Universitas Indonesia, Depok