ANALISIS RISIKO IMPLEMENTASI TI MENGGUNAKAN COBIT 4.1 (STUDI KASUS: STMIK DUTA BANGSA SURAKARTA)

Oleh :
Intan Oktaviani, Manik Hapsara, Emha Taufiq Luthfi
STMIK AMIKOM YOGYAKARTA

ABSTRAK

Sering terjadinya gangguan dan tingkat keamanan implementasi teknologi informasi yang rendah di STMIK Duta Bangsa sehingga banyak peluang resiko yang dapat terjadi. Dari permasalahan-permasalahan yang sering maka diperlukan analisis risiko bertujuan untuk mengetahui risiko-risiko yang dapat timbul dari keberadaan. sampel penelitiannya. Responden yang terlibat terdiri dari Ketua, Wakil Ketua I, Wakil Ketua II, Wakil Ketua III, Badan Penjaminan Mutu STMIK Duta Bangsa Surakarta.

Setiap pernyataan yang terdapat di dalam kuisioner penulis mengacu kepada kontrol objektif sub dari setiap modul yang terdapat di dalam domain PO1, PO9, AI6, ME1, DS11, DS5 dari framework Cobit. Dalam hal ini, skala Likert yang digunakan ada dalam lima tingkatan bobot yang terdiri dari: Tidak Setuju (bobot = 1), Kurang Setuju (bobot = 2), Tidak Tahu (bobot = 0), Setuju (bobot = 4), dan Sangat Setuju (bobot = 5).

Hasil dari rata-rata maturity level didapatkan pada penyebaran kuisoner per domain bahwa berada pada level 2 (Repeatable) yaitu kondisi di mana STMIK Duta Bangsa telah memiliki aturan dalam melakukan tatakelola TI, namun aktifitasnya belum terdefinisi dan terdokumentasi dengan baik secara formal sehingga belum konsisten dilakukan

Kata kunci: Framework Cobit 4.1, Domain, Risiko, Kuisoner, Likert, Maturity

PENDAHULUAN

Sering terjadinya gangguan dan tingkat keamanan implementasi teknologi informasi yang rendah di STMIK Duta Bangsa sehingga banyak peluang resiko yang dapat terjadi. Sebagai contoh dari gangguan dari implementasi teknologi informasi yang sering terjadi di STMIK Duta Bangsa adalah belum terdapat passoword pada komputer server pengelolaan sistem informasi akademik, sehingga dari kurang terjaganya kerahasiaan pada data. Selain hal tersebut, hal yang mendasari dari penelitian ini adalah banyaknya intensitas komplain oleh petugas administrasi karena hanya terdapat satu user dan password yang digunakan pada aplikasi sistem informasi dan ada lebih dari satu petugas administrasi yang mengelola, sehingga apabila terjadi kesalahan baik pada input data maupun proses susah untuk melacaknya. Dari permasalahan-permasalahan yang sering muncul di STMIK Duta Bangsa, maka diperlukan analisis risiko bertujuan untuk

mengetahui risiko-risiko yang dapat timbul dari keberadaan implementasinya. Berikut tabel implementasi teknologi informasi di STMIK Duta Bangsa Surakara :

Tabel 1.1. Implementasi teknologi informasi di STMIK Duta Bangsa.
Sumber : Arsip Staf TI STMIK Duta Bangsa.

No	Tahun	Jum Implementasi TI	Berhasil	Gagal	% Berhasil	% Gagal
1	2011	4	1	3	25%	75%
2	2012	7	2	5	29%	71%
3	2013	3	2	1	67%	33%
4	2014	6	2	4	33%	67%

Tabel dan grafik diatas penggambarkan bahwa dari tahun 2011 sampai tahun 2014 risiko kegagalan terhadap implementasi teknologi informasi masih terbilang tinggi, terbukti hanya pada tahun 2013 implementasi teknologi informasi mengalami prosentase keberhasilan yang lebih tinggi dibanding dengan prosentasi kegagalan. (Arsip staf TI STMIK Duta Bangsa 2014)

Pentingnya analisis risiko terhadap implementasi TI yang menunjang dalam ketercapaiannya visi dan misi institusi, mendorong penulis untuk meneliti lebih lanjut terhadap risiko yang akan muncul dari implementasi TI pada STMIK Duta Bangsa Surakarta.

TINJAUAN TEORI

Analisis merupakan sebuah kegiatan untuk meneliti suatu objek tertentu secara sistematis, guna mendapatkan informasi mengenai objek tersebut.

Menurut Darminto dan Julianty (2002;52) Analisis dapat diartikan sebagai penguraian suatu pokok atas berbagai bagiannya dan penelaahan bagian itu sendiri, serta hubungan antar bagian untuk memperoleh pengertian yang tepat dan pemahaman arti keseluruhan.

Menurut Syahrul dan Nizar (2000;48) Analisis adalah melakukan evaluasi terhadap kondisi dari pos-pos atau ayat-ayat yang berkaitan dengan akuntansi dan alasan-alasan yang memungkinkan tentang perbedaan yang muncul.

Enterprise Risk Management (*ERM*) adalah suatu proses yang berpengaruh pada sebuah entitas, jajaran direksi, pihak manajemen, dan personel lain yang diaplikasikan pada penetapan strategy perusahaan, didisain untuk mengidentifikasi kejadian yang potensial yang dapat berpengaruh pada entitas, dan mengelola risiko yang dapat diterima, dan memberikan jaminan keamanan yang beralasan dalam rangaka mencapai tujuan perusahaan. (*COSO Enterprise Risk Management – Integrated Framework. 2004. COSO)*

Resiko merupakan peluang terjadinya sesuatu yang akan mempunyai dampak terhadap sasaran. Vaughan yang diterjemahkan oleh Herman Darmawi (1997: 18) mengemukakan beberapa definisi risiko sebagai berikut:

a. *Risk is the chance of loss* (risiko adalah kans kerugian).

Chance of Loss biasanya dipergunakan untuk menunjukkan suatu keadaan dimana terdapat suatu keterbukaan terhadap kerugian atau suatu kemungkinan Kerugian. sebaliknya jika disesuaikan dengan istilah yang dipakai dalam statistik, maka *chance* sering dipergunakan untuk menunjukkan tingkat probabilitas akan munculnya situasi tertentu.

b. *Risk is the possibility of loss* (risiko adalah kemungkinan kerugian).

Istilah *possibility* berarti bahwa probabilitas sesuatu peristiwa berada di antara nol dan satu. Definisi ini barangkali sangat mendekati dengan pengertian risiko yang dipakai sehari-hari, akan tetapi definisi ini agak longgar, tidak cocok dipakai dalam analisis secara kuantitatif

c. *Risk is uncertainty* (risiko adalah ketidakpastian)

Tampaknya ada kesepakatan bahwa risiko berhubungan dengan ketidakpastian. Karena itulah ada penulis yang mengatakan bahwa risiko itu sama artinya dengan ketidakpastian.

Menurut Jones (2004: 142), risiko adalah kemungkinan pendapatan yang diterima (*actual return*) dalam suatu investasi akan berbeda dengan pendapatan yang diharapkan (*expected return*). Semakin besar penyimpangan antara hasil sesungguhnya dengan hasil yang diharapkan, berarti semakin besar risiko yang akan ditanggung.

Analisa risiko merupakan metode mengidentifikasi risiko dan menilai kerusakan yang mungkin disebabkan, sebagai alasan perlunya perlindungan keamanan.

Analisa risiko memiliki tiga tujuan, yaitu :

a. Mengidentifikasi risiko
b. Menghitung dampak dari ancaman
c. Memberikan perbandingan biaya/ manfaat antara dampak risiko dengan biaya.

Analisa risiko pada umumnya dilakukan setelah melakukan identifikasi terhadap sebuah risiko. Setelah melakukan identifikasi risiko, maka tahap berikutnya adalah pengukuran risiko dengan cara melihat potensial terjadinya seberapa besar *severity* (kerusakan) dan probabilitas terjadinya risiko tersebut. Penentuan probabilitas terjadinya suatu event sangatlah subyektif dan lebih berdasarkan nalar dan pengalaman. Beberapa risiko memang mudah untuk diukur, namun sangatlah sulit untuk memastikan probabilitas suatu kejadian yang sangat jarang terjadi. Sehingga pada tahap ini sangatlah penting untuk menentukan dugaan yang terbaik supaya nantinya kita dapat memprioritaskan dengan baik dalam implementasi perencanaan manajemen risiko. Kesulitan dalam pengukuran risiko adalah menentukan kemungkinan terjadi suatu risiko karena informasi statistik tidak selalu tersedia untuk beberapa risiko tertentu. Selain itu, mengevaluasi dampak *severity* (kerusakan) seringkali cukup sulit untuk asset immateriil.

Kebijakan pengelolaan TI pada umumnya bertujuan untuk memastikan bahwa penyelenggaraan TI dapat mendukung pencapaian rencana bisnis Bank dan memastikan risiko yang terkait baik secara langsung maupun tidak langsung dengan penyelenggaraan TI

tersebut dapat diatasi. Dalam melakukan identifikasi dan penilaian risiko tersebut, manajemen terlebih dahulu harus memastikan adanya *risk awareness*.

Menurut PBI (2007) Untuk itu penilaian risiko yang dilakukan Bank perlu dilakukan secara berkesinambungan dengan suatu siklus yang minimal mencakup empat langkah penting sebagai berikut:

a. Pengumpulan data/ dokumen atas aktivitas terkait TI yang berpotensi menimbulkan atau meningkatkan risiko baik dari kegiatan yang akan maupun sedang berjalan termasuk namun tidak terbatas pada:

1) Aset TI yang kritikal, dalam rangka mengidentifikasi titik-titik akses dan penyimpangan terhadap informasi nasabah yang bersifat rahasia;

2) Hasil *review* rencana strategis bisnis, khususnya *review* terhadap penilaian risiko potensial;

3) Hasil *due dilligence* dan pemantauan terhadap kinerja pihak penyedia jasa;

4) Hasil *review* atas laporan atau keluhan yang disampaikan oleh nasabah dan atau pengguna TI ke *Call Center* dan atau *Help Desk*;

5) Hasil *Self Assessment* yang dilakukan seluruh satuan kerja terhadap pengendalian yang dilakukan terkait TI;

6) Temuan-temuan audit terkait penyelenggaraan dan penggunaan TI.

b. Analisis risiko berkaitan dengan dampak potensial dari tiap-tiap risiko, misalnya dari fraud di pemrograman, virus komputer, kegagalan sistem, bencana alam, kesalahan pemilihan teknologi yang digunakan, masalah pengembangan dan implementasi sistem, kesalahan prediksi perkembangan bisnis Bank.

c. Penetapan prioritas pengendalian dan langkah mitigasi yang didasarkan pada hasil penilaian risiko Bank secara keseluruhan. Untuk itu Bank harus membuat peringkat risiko berdasarkan kemungkinan kejadian dan besarnya dampak yang dapat ditimbulkan serta mitigasi risiko yang dapat dilakukan untuk menurunkan *eksposure* risiko tersebut.

d. Pemantauan kegiatan pengendalian dan mitigasi yang telah dilakukan atas risiko yang diidentifikasi dalam periode penilaian risiko sebelumnya.

COBIT yaitu *Control Objectives for Information and Related Technology* yang merupakan audit sistem informasi dan dasar pengendalian yang dibuat oleh *Information Systems Audit and Control Association* (ISACA), dan *Information Technology Governance Institute (ITGI)* pada tahun 1992. Prinsip dasar COBIT (Simonsson & Johnson, 2006):

a. *Business information requirements*, terdiri dari: *Effectiveness, Efficiency, Integrity, Availability, and Reliability of information*.
b. High-Level IT Processes, terdiri dari: *IT Domains (Planning and Organisation, Acquisition & Implementation, Delivery & Support, Monitoring and Evaluation); IT Process (IT strategy, Computer operations, Incident handling, Acceptance testing, Change management, Contingency planning, Problem management); Activities (Record new problem, Analyse, Propose solution, Monitor solution, Record known problem.).*

c. *Information Technology Resource: Expert staff, Applications, Technology, Facilities, Database Management System, Hardware, Software, Multimedia.*

METODE PENELITIAN

Framework manajemen risiko TI dengan menggunakan COBIT terdiri dari :

a. Penetapan Objektif
   Terdapat tujuh kriteria informasi dari COBIT yaitu : *effectiveness, efficiency, confidentiality, integrity, availability, compliance, dan reliability.*
b. identifikasi Risiko
   Identifikasi risiko merupakan proses untuk mengetahui risiko. Sumber risiko bisa berasal dari :
   1) Manusia, proses dan teknologi
   2) *Internal* (dari dalam perusahaan) dan *eksternal* (dari luar perusahaan)
   3) Bencana
   4) (*hazard*), ketidakpastian (*uncertainty*) dan kesempatan (*opportunity*).
c. Penilaian
   1) Proses untuk menilai seberapa sering risiko terjadi atau seberapa besar dampak dari risiko.
   2) Dampak risiko terhadap bisnis (*business impact*)
   3) Kecenderungan (*likelihood*) terjadinya risiko dapat disebabkan oleh sifat alami dari bisnis, struktur dan budaya organisasi, sifat alami dari sistem (tertutup atau terbuka, teknologi baru dan lama), dan kendali-kendali yang ada.
   4) Proses penilaian risiko bisa berupa risiko yang tidak dapat dipisahkan (i*nherent risks*) dan sisa risiko (*residual risks*).
d. Respon Risiko

Proses-proses pada framework COBIT Versi 4.1 (dari 34 *Control Objectives*) yang sesuai untuk manajemen risiko adalah (ISACA 2008) :

a) PO1 (Define a Stretegic IT Plan) dan PO9 (Assess and Manage Risks)
b) AI6 (Manages Change)
c) DS5 (Ensure System and Security) dan DS11(Manage Data)
d) ME1 (Monitor and Evaluate IT Performance)

e. Monitor Risiko

Setiap langkah dimonitor untuk menjamin bahwa risiko dan respon berjalan sepanjang waktu

Metode Analisis Data

Metode analisis data hasil penelitian ini (yang berupa jawaban kuisioner) dilakukan dengan menggunakan analisis Kemudian untuk sampel penelitiannya, peneliti menggunakan responden yang terdiri dari Ketua, Wakil Ketua I, Wakil Ketua II, Wakil Ketua III, Badan Penjaminan Mutu .

PENGOLAHAN DATA

Teknik pengambilan data dilakukan dengan meminta pihak yang terkait dalam implemntasi TI yaitu dengan mengisi kuisioner. Setiap pernyataan yang terdapat di dalam kuisioner penulis mengacu kepada kontrol objektif sub dari setiap modul yang terdapat di dalam domain PO1, PO9, AI6, ME1, DS11, DS5 dari *framework* Cobit. Kuesioner penelitian ini dapat dilihat pada Lampiran, responden diminta untuk memberikan pendapatnya mengenai keberadaan investasi pada implementasi TI di STMIK Duta Bangsa Surakarta. Dalam hal ini, skala *Likert* yang digunakan ada dalam lima tingkatan bobot yang terdiri dari: Tidak Setuju (bobot = 1), Kurang Setuju (bobot = 2), Tidak Tahu (bobot = 0), Setuju (bobot = 4), dan Sangat Setuju (bobot = 5).

Perhitungan Level Per Domain

Perhitungan level setiap domain didapatkan dari total skor setiap skala dibagi dengan total jumlah pertanyaan setiap level, sehingga apabila total hasil perhitungan setiap level dijumlahkan maka mendapatkan hasil 5,00 yang merupakan jumlah dari responden yang berpartisipasi dalam pengisian kuisoner.

$$\text{Indek Kematangan Atribut} = \frac{\sum (\text{total skor setiap skala})}{\text{jumlah pertanyaan setiap level}}$$

Penghitungan Indeks Kematangan Atribut

$$\text{Indek Kematangan Atribut} = \frac{\sum (\text{total jawaban x bobot})}{\text{Jumlah Responden}}$$

Penghitungan Indeks Kematangan

$$\text{Indek Kematangan Atribut} = \frac{\sum \text{Indek Kematangan Atribut}}{6}$$

ANALISIS HASIL

Hasil dari rata-rata maturity level didapatkan pada penyebaran kuisoner per domain bahwa berada pada level 2 (*Repeatable)* yaitu kondisi di mana STMIK Duta Bangsa telah memiliki aturan dalam melakukan tatakelola TI, namun aktifitasnya belum terdefinisi dan terdokumentasi dengan baik secara formal sehingga belum konsisten dilakukan. (berdasarkan SOP nomor PM-STMIK-DB-1, SOP nomor PM-STMIK-DB-2, SOP nomor PM-STMIK-DB-3, SOP nomor PM-STMIK-DB-4, SOP nomor PM-STMIK-DB-5, SOP nomor PM-STMIK-DB-6, SOP nomor PM-STMIK-DB-18, SOP nomor PM-STMIK-DB-21, SOP nomor PM-STMIK-DB-23, Visi dan Misi poin a, b, c, d, serta Renstra STMIK Duta Bangsa).

Analisis resiko dicoba mengikuti beberapa panduan *dari IT Assurance guide: using COBIT*. Analisis resiko dari STMIK Duta Bangsa Surakartadibagi kedalam penentuan aset yang harus dilindungi, ancaman dan resiko yang terjadi bila aset tersebut tidak memiliki kontrol yang layak. Guna untuk mewujudkan Visi , Misi dan Rencana Srategis STMIK Duta Bangsa Surakarta.

.

KESIMPULAN

Hasil kuisoner dari setiap *control practise* memberikan jawaban berdasarkan *maturity* di STMIK Duta Bangsa. Analisa resiko diperlukan guna untuk mengetahui resiko-resiko apa saja yang akan muncul dari keberadaan TI di STMIK Duta Bangsa Surakarta. Hasil dari rata-rata maturity level didapatkan pada penyebaran kuisoner per domain bahwa berada pada level 2 (*Repeatable)* yaitu kondisi di mana STMIK Duta Bangsa telah memiliki aturan dalam melakukan tatakelola TI, namun aktifitasnya belum terdefinisi dan terdokumentasi dengan baik secara formal sehingga belum konsisten dilakukan.

DAFTAR PUSTAKA

BANK Indonesia. 2007. *Pedoman Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh BANK Umum*. Lampiran Surat Edaran Bank Indonesia.

COBIT 4.1. 2007. ISACA. IT Governance Institute.

COBIT FOCUS. 2008. ISACA. IT Governance Institute

Fletcher, Matthew.2006. *Five Domains of Information Technology Governance for Consideration by Boards of Directors.* Portland : Information Management Program University of Oregon.

ISO 9241-210 2010. *Human-Centred Design Process for Interactive Systems, International Organization for Standardization.* Geneve.

[ITGI] *IT Governance Institute*. 2003. *IT Control Objectives for Sarbanes–Oxley:The Role of IT in the Design and Implementation of Internal Control OverFinancial Reporting, 2nd Edition. Rolling Meadows, IL: IT GovernanceInstitute.*

[ITGI] *IT Governance Institute*. 2006. *COBIT MAPPING Overview International IT Guidance, 2nd Edition. IT Governance Insitute*

[ITGI] *IT Governance Institute. 2007. COBIT® 4.1. IT Governance Insitute.*

Rencana Startegi. 2012. Surakarta: STMIK Duta Bangsa

Standar Operasional Prosedur. 2012. Surakarta: STMIK Duta Bangsa

Surendro. Kridanto, 2009, *Implementasi Tata Kelola Teknologi Informasi, Informatika, Bandung.*

Visi dan Misi. 2012. Surakarta: STMIK Duta Bangsa

Tim Direktorat keamanan Informasi. 2011. *Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik.* Kementerian Komunikasi dan Informatika RI.

Jogiyanto HM. 2011. *Sistem Tata Kelola Teknologi Informasi.* Yogyakarta :Andi.

Champlain, Jack J. *Auditing Information System: A Comprehensive Reference Guide*. New York: John Wiley & Son, 1998.

Finney, Sherry, dkk. 2007. *ERP implementation: a compilation and analysis of critical success factor. Emerald Group Publishing Limited.*

Gomes R, Riberio J. *2009. The Main Benefits Of Cobit In A High Public Educational Institution - A Case Study. Proceedings of Pacific Asia Conference on Information Systems; 2009. Association fo Information System. 2009*. hlm 0 -12.

Jakaria, Deni Ahmad, dkk. 2013. *Manajemen Risiko Sistem informasi Akademik pada Perguruan Tinggi Menggunakan Metode Octave Allegro.* Yogyakarta : Seminar Nasional Aplikasi Teknologi Infromasi (SNATI).

Kania, W._201. *Pengukuran Tingkat Kemapanan Penerapan Teknologi Rfid Di Perpustakaan Nasional Ri Berdasarkan Framework COBIT 4.1.* Pascasarjana IPB.

Kesumawardhani. *2012. Evaluasi It Governance Berdasarkan COBIT 4.1 (STUDI KASUS DI PT TIMAH (PERSERO) Tbk).*

Kurniawan. 2012. *Sistem Informasi Sumber Daya Manusia Bagi Perguruan Tinggi Swasta (Studi Kasus Universitas Bina Darma)*. Yogyakarta : semnasIF.

Nurhidayat, Boyke. 2011. *Evaluasi Integrated Toll Collection System Dengan Menggunakan Framework Cobit*. Bogor: Institut Pertanian Bogor.

Mapping, C. 2011. *COBIT Mapping. Overview of International IT Guidance 3nd edition.*

Razali, Ahmad, dkk. 2011. *Review of literatue on Enterprise Risk Management*. Business Management Dynamics.

Sarno, R.. 2009. *Audit Sistem & Teknologi Informasi*. ITS Press. Surabaya

Salahuddin Al Arif. 2011. *Perancangan Tata Kelola Teknologi Informasi Studi Kasus : PT XYZ Indonesia.*

Setiawan , A. 2008. *Evaluasi Penerapan Teknologi Informasi Di Perguruan Tinggi Swasta Yogyakarta Dengan Menggunakan Model Cobit Framework.* Seminar Nasional Aplikasi Teknologi Informasi.

Setiawan , A. 2010. *Pengaruh Kematangan, Kinerja Dan Perkembangan Teknologi Informasi Di Perguruan Tinggi Swasta Yogyakarta Dengan Model Cobit Framework*. Seminar Nasional Informatika.

Simonsson , M. 2008. *Predicting It Governance Performance: A Method For Model-Based Decision Making* .

Simonsson , M., & Johnson , P. 2005. *Defining It Governance A Consolidation Of Literature* .

Simonsson , M., & Johnson , P. 2006. *Assessment of IT Governance – A Prioritization of Cobit* -. *151*.

Simonsson, M., & Nordstram, L. 2008. *Modelling and Evaluating the Maturity of ICT Governance Processes in the Power Industry. SC D2 Information Systems and Telecommunications.*

Simonsson, M., Johnson, P., & Wijkström, H. 2006. *Model-Based It Governance Maturity Assessments With Cobit.*

Supradono, Bambang. 2009. *Manajemen Risiko Keamanan Informasi Dengan menggunakan Metode OCTAVE.* Media Elektrika, Vol. 2, No. 1: 4-8.

Wardhani, Karina.2011. *Manajemen Risiko dan Implementasinya Dalam Sistem Informasi.* Bandung : Makalah II2092 Probabilitas dan Statistik – Sem. I.

PUSTAKA ELEKTRONIK

http://stmikdb.ac.id/news.php