Tingkat Kematangan Tata Kelola Teknologi Informasi Untuk Praktik Kendali Instalasi dan Akreditasi Sistem *(Cobit Ai 5) Control Objective* Pengujian Keamanan Akreditasi dan Uji operacional (Studi Kasus Pt Xyz Indonesia)

The Maturity Level of Operating Informatic Technology to Practice Installation Control and Accredited System (Cobit Ai 5) of Control Objective of Accredited SecurityAnd Operational Testing (Case Study in PT XYZ Indonesia)

Rima Maulini 1)

1) *Staf Pengajar Program Studi Manajemen Informasi Jurusan Ekonomi dan Bisnis Politeknik Negeri Lampung*

ABSTRACT

Installation processes, testing and receiving system are less formulated even though they were done. Formation gives big effect to develop informatics technology (IT) which support the use of IT to reach business aims. The aims of operating AI 5 are: To do verification and confirm that a solution was relevant to the needed aims through realization of formulated planning about installation, migration, convertion, and acceptance. By using COBIT audit methodology, was well known the maturity level of operating informatics technology to practice control installation and accredited system (cobit ai 5) of control objective of accredited security and operational testing for each controlling item on position 3 (determined process) and position 4 (can be regulated and measured)

Key words: Audit, Cobit, operating

Pendahuluan

Peranan teknologi informasi semakin kuat dalam mendukung organisasi mencapai tujuannya. Sebagai konsekuensinya, perkembangan bisnis organisasi dan perubahan yang dijalaninya memberikan dampak pada TI, di lain sisi TI sendiri semakin diharapkan untuk menjadi wahana yang membantu transformasi tersebut. Apabila perkembangan tidak dikelola dan ditanggapi dengan cepat serta efektif, maka gelaran perubahan tidak membawa keuntungan bagi organisasi tersebut. PT XYZ berupaya untuk menanggapi perkembangan bisnis tersebut dengan mendayagunakan teknologi informasi untuk pengembangan dan diversifikasi berbagai layanannya. Kerja sama strategis dengan mitra-mitra dalam dan luar negeri ditumbuhkan dan dipelihara juga dengan peran kuat dari teknologi informasi.

Seiring dengan dinamika tersebut, maka kebutuhan akan sistem aplikasi semakin meningkat yang diiringi siklus hidup sistem aplikasi tersebut bergulir dengan cepat. Selain analisis dan perancangan sistem aplikasi yang harus efektif dan memberikan hasil yang sesuai dengan *arsitektur enterprise* PT XYZ, selanjutnya yaitu pemasangan, pengujian dan penerimaan sistem aplikasi juga menjadi penentu kesuksesan.

Proses-proses pemasangan, pengujian dan penerimaan sistem cenderung kurang diformalisasikan walaupun banyak dilakukan. Formalisasi memberikan dampak besar dalam membangun tata kelola TI yang menunjang pemanfaatan TI untuk pencapaian tujuan bisnis.

Dalam standar *Control Objective for Information and Related Technology* (COBIT), praktik kendali perlu dinyatakan secara formal untuk perwujudan struktur kendali yang efektif. Untuk proses-proses di atas, COBIT menyediakan domain Akuisisi dan Implementasi (AI) pada proses Instalasi dan Akreditas atas Sistem (AI 5). Organisasi yang telah sukses mengimplementasikan instalasi dan akreditas dari sistem-sistem melaporkan keuntungan-keuntungan sebagai berikut:

a. Jumlah perubahan yang diperlukan semakin terminimasi setelah solusi mulai direalisasikan dan diproduksi;
b. Semakin berkurangnya milestone yang terlewatkan dalam instalasi dan akreditas; dan
c. Waktu yang lebih optimal dalam menyelesaikan proses-proses instalasi dan akreditasi.

Tujuan kendali AI 5 adalah: melakukan verifikasi dan mengkonfirmasikan bahwa suatu solusi adalah sesuai dengan tujuan yang diinginkan melalui realisasi atas rencana yang terformalisasi dengan baik mengenai instalasi, migrasi, konversi dan penerimaan. Kajian ini bertujuan untuk mengumpulkan data dan menerapkan analisis untuk meninjau tingkat kedewasaan (*maturity level*) dan kepatuhannya dalam tata kelola TI untuk *control objective* Pengujian Keamanan dan Akreditasi dan Uji Operasional serta menghasilkan evaluasi awal atas tingkat kedewasaan tata kelola TI dan kepatuhannya, secara khusus untuk proses dan praktik kendali AI 5 Instalasi dan Akreditasi Sistem untuk *control objective* Pengujian keamanan dan akreditasi dan Uji operasional. Hasil - hasil evaluasi kemudian dikembangkan untuk menghasilkan masukan-masukan awal untuk peningkatan efektivitas tata kelola TI untuk semakin menunjang keselarasan antara TI dan pencapaian tujuan bisnis.

Kerangka Teoritis

Framework COBIT

Control Objectives for Information and related Technology (COBIT) adalah sekumpulan dokumentasi *best practices* untuk *IT governance* yang dapat membantu auditor, manajemen dan pengguna (*user*) untuk menjembatani gap antara risiko bisnis, kebutuhan kontrol dan permasalahan-permasalahan teknis (COBIT, 2003)

COBIT dikembangkan oleh IT Governance Institute, yang merupakan bagian dari *Information Systems Audit and Control Association* (ISACA). COBIT memberikan arahan (*guidelines*) yang berorientasi pada bisnis, dan karena itu *business process owners* dan manajer, termasuk juga auditor dan *user*, diharapkan dapat memanfaatkan *guideline* ini dengan sebaik-baiknya. Kerangka kerja COBIT ini terdiri atas beberapa arahan (*guidelines*), yakni:

Control Objectives: Terdiri atas 4 tujuan pengendalian tingkat-tinggi (*high-level control objectives*) yang tercermin dalam 4 domain, yaitu: *planning & organization* , *acquisition & implementation* , *delivery & support* , dan *monitoring* .

Audit Guidelines: Berisi sebanyak 318 tujuan-tujuan pengendalian yang bersifat rinci (*detailed control objectives*) untuk membantu para auditor dalam memberikan *management assurance* dan atau saran perbaikan.

Management Guidelines: Berisi arahan, baik secara umum maupun spesifik, mengenai apa saja yang mesti dilakukan, terutama agar dapat menjawab pertanyaan-pertanyaan berikut:

a) Sejauh mana Anda (TI) harus bergerak, dan apakah biaya TI yang dikeluarkan sesuai dengan manfaat yang dihasilkannya.
b) Apa saja indikator untuk suatu kinerja yang bagus?
c) Apa saja faktor atau kondisi yang harus diciptakan agar dapat mencapai sukses (*critical success factors*)?
d) Apa saja risiko-risiko yang timbul, apabila kita tidak mencapai sasaran yang ditentukan?
e) Bagaimana dengan perusahaan lainnya – apa yang mereka lakukan?
f) Bagaimana Anda mengukur keberhasilan dan bagaimana pula membandingkannya.

The COBIT Framework memasukkan juga hal-hal berikut ini:

a) *Maturity Models* – Untuk memetakan status maturity proses-proses TI (dalam skala 0 – 5) *dibandingkan dengan "the best in the class in the Industry"* dan juga International best practices
b) *Critical Success Factors* (CSFs) – Arahan implementasi bagi manajemen agar dapat melakukan kontrol atas proses TI.
c) *Key Goal Indicators* (KGIs) – Kinerja proses-proses TI sehubungan dengan business requirements
d) *Key Performance Indicators* (KPIs) – Kinerja proses-proses TI sehubungan dengan *process goals.*

COBIT dikembangkan sebagai suatu *generally applicable and accepted standard for good Information Technology (IT) security and control practices* . Istilah " *generally applicable and accepted* " digunakan secara eksplisit dalam pengertian yang sama seperti *Generally Accepted Accounting Principles* (GAAP) (COBIT, 2003).

Sedang, COBIT's "good practices" mencerminkan konsensus antar para ahli di seluruh dunia. COBIT dapat digunakan sebagai IT *Governance tools*, dan juga membantu perusahaan

mengoptimalkan investasi TI mereka. Hal penting lainnya, COBIT dapat juga dijadikan sebagai acuan atau referensi apabila terjadi suatu kesimpang-siuran dalam penerapan teknologi.

Suatu perencanaan Audit Sistem Informasi berbasis teknologi (audit TI) oleh Internal Auditor, dapat dimulai dengan menentukan area-area yang relevan dan berisiko paling tinggi, melalui analisa atas ke-34 proses tersebut. Sementara untuk kebutuhan penugasan tertentu, misalnya audit atas proyek TI, dapat dimulai dengan memilih proses yang relevan dari proses-proses tersebut (Henczel, 2001). Selain dapat digunakan oleh Auditor, COBIT dapat juga digunakan oleh manajemen sebagai jembatan antara risiko-risiko TI dengan pengendalian yang dibutuhkan (IT *risk management*) dan juga referensi utama yang sangat membantu dalam penerapan IT *Governance* di perusahaan (COBIT, 2003).

Metode Kajian

Auditors

Merupakan alat yang digunakan melakukan proses audit, dalam hal ini digunakan ***Certified Information Systems Auditor*** (CISA)**.** Program CISA didesain untuk menilai dan menjamin organisasi dalam audit sistem informasi, kontrol dan tugas-tugas keamanan.

Cobit

Merupakan program standar untuk membantu dalam menemukan kebutuhan pihak manajemen dengan menjembatani jarak antara resiko bisnis, kebutuhan kontrol dan isu-isu teknik. COBIT juga menawarkan praktik terbaik melalui *framework domain* dan proses dan aktivitas sekarang yang dapat diatur dan dikendalikan.COBIT merupakan persetujuan dari para ahli yang akan membantu dalam mengoptimalisasi investasi informasi dan akan menawarkan ukuran yang harus diperbaiki ketika apa yang organisasi lakukan menemui kesalahan/kegagalan.

Metode Audit

Tahapan-tahapan yang dalam melakukan proses audit yaitu :

a. Studi pustaka atas standar COBIT untuk memahami tata kelola TI melalui COBIT.
b. Pengolahan COBIT AI 5 lebih lanjut untuk menghasilkan butir-butir periksa untuk pengambilan data lebih lanjut.
c. Pengambilan data dengan kunjungan ke kantor PT XYZ, wawancara dan diskusi dengan personil PT XYZ.
d. Pengolahan data (butir-butir periksa) untuk menghasilkan kuantifikasi estimasi tingkat kedewasaan tata kelola TI dan kepatuhannya, yang bersifat sementara.
e. Penyusunan laporan dan rekomendasi berdasarkan hasil-hasil terdahulu.

Sedangkan langkah-langkah audit di PT XYZ dilakukan sebagai berikut:

1) Menentukan *Critical Succes Factor* (CFS) PT XYZ .

CSF PT XYZ berdasarkan identifikasi yang dilakukan adalah sebagai berikut:

a. Komitmen dan konsistensi *Board of Directors* (BOD), mutlak diperlukan untuk menjamin implementasi RSTI (Rencana Strategis Teknologi Informasi) sesuai dengan konsep yang telah dibuat.
b. Komitmen dan konsistensi serta penguasaan para GM, Manajer dan tenaga IT terhadap implementasi RSTI.
c. Audiat TI PT. XYZ harus jalan dengan kondisi jaringan virtual yang ada dan mengantisipasi perkembangan telematika masa depan.
d. Arsitektur harus memberi standar untuk pembangunan ke depan.
e. Arsitektur harus menyediakan dukungan bagi manajemen untuk ekspansi di area jaringan dan e-commerce
f. Arsitektur harus memberikan dukungan operasional bisnis PT. XYZ.
g. Arsitektur harus dapat mewadahi kebutuhan interkoneksi dengan standar transaksi yang telah berjalan, seperti EDI, Messaging (ISO,XML,dll), WAP dan standar lainnya.
h. Arsitektur harus dapat membangun dan meningkatkan kemampuan SDM XYZ.

2) COBIT AI5:

a. Control Objective : Pengujian keamanan dan akreditasi

Pihak manajemen seharusnya dapat mengidentifikasi dan mengimplementasikan prosedur-prosedur untuk meyakinkan bahwa manejemen pengguna dan operasi secara resmi dapat menerima hasil pengujian dan tingkat keamanan untuk sistem sejalan dengan sisa resiko yang masih ada. Prosedur ini seharusnya dapat merefleksikan persetujuan dalam aturan-aturan dan tanggung jawab dari pengguna, pengembang sistem, manajemen jaringan dan personel sistem operasi, yang diambil dari pemisahan account, supervisi dan pengawasan isu-isu.

b. Control Objective : Uji operasional

Pihak manajemen seharusnya dapat meyakinkan bahwa sebelum memindahkan sistem ke dalam operasi, pengguna mengesahkan operasi tersebut sebagai suatu produk yang lengkap, dalam kondisi serupa dengan lingkungan aplikasi dan dengan cara yang mana sistem tersebut akan dijalankan dalam lingkungan produksi.

3) Butir-butir periksa : Pengujian keamanan dan akreditasi dan Uji Operasional, yang meliputi pertanyaan-pertanyaan:

a. Apakah mekanisme penetapan dan dokumentasi dalam tahap penetapan kebutuhan '*security'* dan pengendalian internal ditetapkan untuk pengujian keamanan dan akreditasi?
b. Dalam tahap realisasi (baik dalam upaya pengembangan sistem aplikasi secara mandiri ataupun dalam kerja sama dengan pihak luar, misalnya vendor, kontraktor atau pengembang lainnya), apakah instansi anda melakukan pengendalian atas

pengembangan/pembuatan sistem aplikasi sehingga pihak-pihak kunci (pengguna, manajemen TI, dsb) tetap dapat melakukan pemantauan dan dapat memberikan umpan balik agar sistem sesuai dengan kebutuhan?

c. Apakah peranan '*security'* dan pengendalian internal dalam mengawasi jalannya penggunaan sistem ditetapkan dalam uji operasional?

d. Apakah tersedia rencana pengujian yang mencakup semua bidang sumber daya sistem informasi: software aplikasi, fasilitas, teknologi dan pemakai?

Butir-butir periksa diatas kemudian akan diberikan penilaian dengan standar penilaian yang ada pada standar COBIT pada butir periksa ini, dengan kriteria sebagai berikut:

- 5 = Optimize
- 4 = Diatur dan Dapat Diukur
- 3 = Proses Ditetapkan
- 2 = Terdefinisi
- 1 = Tidak Kenal

Hasil dan Pembahasan

Hasil kuesioner dan pengolahannya lebih lanjut memberikan kuantifikasi, ditunjukkan pada Tabel 1.

Tabel 1. Hasil Butir Periksa PT.XYZ

Bukti periksa	**Jawaban / Nilai**				
Pengujian Keamanan dan Akreditasi	**5**	**4**	**3**	**2**	**1**
▪ Apakah mekanisme penetapan dan dokumentasi dalam tahap penetapan kebutuhan '*security'* dan pengendalian internal ditetapkan untuk pengujian keamanan dan akreditasi?		X			
▪ Dalam tahap realisasi (baik dalam upaya pengembangan sistem aplikasi secara mandiri ataupun dalam kerja sama dengan pihak luar, misalnya vendor, kontraktor atau pengembang lainnya), apakah instansi anda melakukan pengendalian atas pengembangan/pembuatan sistem aplikasi sehingga pihak-pihak kunci (pengguna, manajemen TI, dsb) tetap dapat melakukan pemantauan dan dapat memberikan umpan balik agar sistem sesuai dengan kebutuhan?			X		
Uji Operasional					
▪ Apakah peranan '*security'* dan pengendalian internal dalam mengawasi jalannya penggunaan sistem ditetapkan dalam uji operasional sistem?			X		
▪ Apakah tersedia rencana pengujian yang mencakup semua bidang sumber daya sistem informasi: software aplikasi, fasilitas, teknologi dan pemakai?		X			
	-	2	2	**-**	**-**

Berdasarkan Tabel 1, dapat dilihat bahwa PT. XYZ dalam penerapan Tata Kelola TI yaitu untuk Instalasi dan Akreditasi Sistem pada kontrol pengujian keamanan dan akreditasi dan uji operasional berada pada tingkat kedewasaan diposisi 4 dan 3 atau Diatur dan Dapat Diukur dan Proses

Ditetapkan. Dari hasil ini masih menunjukkan bahwa PT. XYZ masih perlu melakukan peningkatan beberapa proses perbaikan terutama yang masih berada pada tingkat kedewasaan 3.

Kesimpulan

Setelah melaksanakan studi, kemudian melakukan pengolahan data untuk tingkat kedewasaannya, maka dapat disimpulkan bahwa PT XYZ dalam melaksanakan salah satu bagian Tata Kelola TI yaitu Instalasi dan Akreditasi Sistem untuk *control objective* Pengujian keamanan dan akreditasi dan Uji operasional dapat disimpulkan sebagai berikut:

a. Pada *control objective* Pengujian keamanan dan akreditasi untuk butir periksa satu tingkat kedewasaannya berada pada diposisi **4** (**Diatur dan Dapat Diukur)**.
b. Pada *control objective* Pengujian keamanan dan akreditasi untuk butir periksa dua tingkat kedewasaannya berada pada diposisi **3** (**Proses Ditetapkan)**.
c. Pada *control objective* Uji Operasional untuk butir periksa satu tingkat kedewasaannya berada pada diposisi **3** (**Proses Ditetapkan)**.
d. Pada *control objective* Uji Operasional untuk butir periksa dua tingkat kedewasaannya berada pada diposisi **4** (**Diatur dan Dapat Diukur)**.

Daftar Pustaka

Cobit 4.1, 2003., *Management Guideline* : *How to Implement COBIT 4.1 in Enterprise Information Technology*

Ennis, Kathy, 2000,. *Guideline for Learning Resource and Services in Further and Higher Education: Performance and Resources*. London: Library Association Publishing.

Henczel, Susan. 2001., *The Information Audit: a Practical Guide*. Munchen: Saur.