AUDIT SISTEM INFORMASI/TEKNOLOGI INFORMASI DENGAN KERANGKA KERJA COBIT UNTUK EVALUASI MANAJEMEN TEKNOLOGI INFORMASI DI UNIVERSITAS XYZ

Devi Fitrianah[1] dan Yudho Giri Sucahyo[2]

[1]Fakultas Ilmu Komputer, Universitas Mercu Buana, Indonesia
devi_fitrianah@yahoo.com
[2]Fakultas Ilmu Komputer, Universitas Indonesia, Depok, Indonesia
yudho@cs.ui.ac.id

Abstrak

Pemanfaatan Teknologi Informasi sebagai pendukung pencapaian tujuan dan sasaran organisasi harus diimbangi dengan keefektifan dan efisiensi pengelolaannya. Maka dari itu, audit TI haruslah dilakukan untuk menjaga keamanan sistem informasi sebagai aset organisasi, untuk mempertahankan integritas informasi yang disimpan dan diolah dan tentu saja untuk meningkatkan keefektifan penggunaan teknologi informasi serta mendukung efisiensi dalam organisasi. Penelitian ini bertujuan untuk melakukan pemetaan terhadap tahap audit TI beserta kontrolnya yang kemudian diaplikasikan pada sebuah organisasi, yaitu Universitas XYZ untuk melihat kinerja TI yang ada. Kerangka kerja yang digunakan sebagai acuan adalah COBIT-ISACA dengan menggunakan 210 *detailed control objective* yang ada. Penyelenggaraan audit dilakukan dengan menggunakan tahapan-tahapan yang ada pada *IT Assurance Guide*. Hasil dari evaluasi atau temuan dilakukan analisa *root cause* sehingga didapat sebuah rekomendasi untuk manajemen TI yang lebih baik lagi.

Kata kunci: Audit TI, *control objective*.

1. Pendahuluan

Pemenuhan kebutuhan akan sistem informasi bagi semua jenis organisasi menyebabkan perkembangan sistem informasi yang begitu pesat. Begitu pula dengan perkembangan di sektor pelayanan pendidikan yang dikenal dengan Sistem Informasi Akademik.

Sistem Informasi Akademik merupakan suatu kebutuhan yang mutlak bagi pelayanan pendidikan terutama pada perguruan tinggi, sehingga dapat memberikan kemudahan dalam administrasi bagi perguruan tinggi yang menerapkannya. Dengan adanya Sistem Informasi Akademik dan Sistem Informasi lainnya di universitas XYZ, bukan hanya pelayanan terhadap mahasiswa yang menjadi lebih baik tetapi juga pelayanan untuk seluruh pihak terkait dengan proses akademik yang ada seperti staf pengajar, biro administrasi bahkan orangtua dan alumni. Peranan Sistem Informasi yang signifikan inilah yang tentu saja harus diimbangi dengan pengaturan dan pengelolaan yang tepat sehingga kerugian–kerugian yang mungkin terjadi dapat dihindari. Kerugian yang dimaksud bisa dalam bentuk informasi yang tidak akurat yang disebabkan oleh pemrosesan data yang salah sehingga dapat mempengaruhi pengambilan keputusan yang salah pula. Keamanan asetnya salah satunya adalah data tidak terjaga, integritas data yang tidak dapat dipertahankan, hal–hal inilah yang dapat mempengaruhi efektifitas dan efisiensi dalam pencapaian tujuan dan strategi organisasi.

Sehubungan dengan alasan tersebut diperlukan adanya sebuah mekanisme kontrol terhadap pengelolaan teknologi informasi [1]. Masalah yang sering timbul di Universitas XYZ adalah adanya kasus kehilangan data, kesalahan dalam pengambilan keputusan, kebocoran data, penyalahgunaan komputer dan nilai investigasi TI yang tinggi tetapi tidak diimbangi dengan pengembalian nilai yang sesuai. Berawal dari sini maka diperlukan sebuah mekanisme kontrol atau audit Sistem Informasi atau audit Teknologi Informasi. Audit SI/TI dalam kerangka kerja COBIT lebih sering disebut dengan istilah *IT Assurance* ini bukan hanya dapat memberikan evaluasi terhadap keadaan tata kelola Teknologi Informasi di unversitas XYZ tetapi dapat juga memberikan masukan yang dapat digunakan untuk perbaikan pengelolaannya di masa yang akan datang.

Tujuan dan manfaat dari penelitian ini adalah (1) Melakukan evaluasi terhadap pengelolaan teknologi informasi atau manajemen teknologi informasi yang ada di universitas XYZ. (2) Hasil yang diperoleh dari kajian ini diharapkan dapat dijadikan landasan dalam pembuatan kerangka kerja tata kelola TI yang sesuai dengan standar.

Berdasarkan uraian dari latar belakang permasalahan diatas penulis dapat merumuskan permasalahan penelitian sebagai berikut: (1) Jenis evaluasi manajemen TI yang sesuai untuk organisasi seperti Universitas XYZ. (2) Kontrol objektif yang digunakan dalam melakukan evaluasi.

Penelitian ini difokuskan untuk melakukan evaluasi terhadap pengelolaan teknologi informasi yang mengacu pada proses pelaksanaan di Universitas XYZ dengan menerapkan *IT assurance* yang berbasis kepada *control objective* yang ada pada COBIT versi 4.1 [2].

2. Metodologi Audit SI/TI

Dalam melaksanakan audit TI diterapkan metodologi audit TI yang sesuai dengan metodologi yang diajukan oleh *IT Assurance Guide: Using COBIT*. Tetapi sebelum menentukan pilihan menggunakan COBIT sebagai kerangka kerja audit, dilakukan beberapa pertimbangan diantaranya yaitu dengan melakukan *benchmarking* antara kerangka kerja audit yang ada seperti Ron Weber [1], *Queensland Audit Office* dan Jack Champlain [3]. Semua kerangka audit tersebut dipetakan sehingga didapat sebuah kesimpulan bahwa kerangka COBIT adalah kerangka kerja audit yang paling lengkap. Kemudian penulis juga melakukan perbandingan antara COBIT dengan ITIL (*Information Technology Infrastructure Library*) [4] untuk mendapatkan gambaran yang lebih jelas dalam proses pada domain *Delivery and Support*.

Dalam melaksanakan tahapan audit, tidak semua langkah yang ada didalam panduan tersebut dilaksanakan semuanya, dengan alasan mengurangi pengulangan aktivitas, maka tetap berpegang pada aturan-aturan yang bersifat umum yang telah ditetapkan oleh *IT Assurance Guide* [5].

Pada dasarnya dalam metodologi audit/*assurance*, dilakukan metodologi pengumpulan data, yang meliputi:

i. Penelaahan dokumentasi kebijakan teknik maupun non-teknis yang menjadi dasar pengembangan Universitas XYZ.
ii. Observasi dan wawancara dengan pihak terkait, wawancara dilakukan dengan pihak terkait yaitu kepala pusat Unit Cybernet, kepala pusat pengembangan sistem, staf Cybernet, Direktur Akademik, staf pengajar dan mahasiswa.
iii. Analisa basis data.
iv. Analisa jaringan.

Dalam melaksanakan evaluasi, dilakukan beberapa langkah, yaitu:

a. Penentuan Rencana Audit

Dalam penentuan rencana audit, terdapat langkah-langkah yang dilakukan, yaitu:

1. Memahami visi dan misi dari Universitas XYZ, sasaran, tujuan dan prosesnya.
2. Mengidentifikasi kebijakan, standar, pedoman serta prosedur dari Universitas XYZ.
3. Melakukan analisis resiko.

b. Menentukan lingkup audit dan tujuan audit

Dalam menentukan lingkup audit dan tujuan audit penulis melakukan hal-hal berikut:

1. Menentukan tujuan audit TI.
2. Melakukan pemilihan *control objective* yang akan digunakan untuk menguji keefektifan dari proses TI yang ada.
3. Mendokumentasikan arsitektur yang ada di Universitas XYZ.
4. Mendefinisikan proses-proses TI yang akan dikaji.
5. Mendefinisikan komponen TI yang ada di Universitas XYZ.

c. Melakukan kajian di universitas XYZ

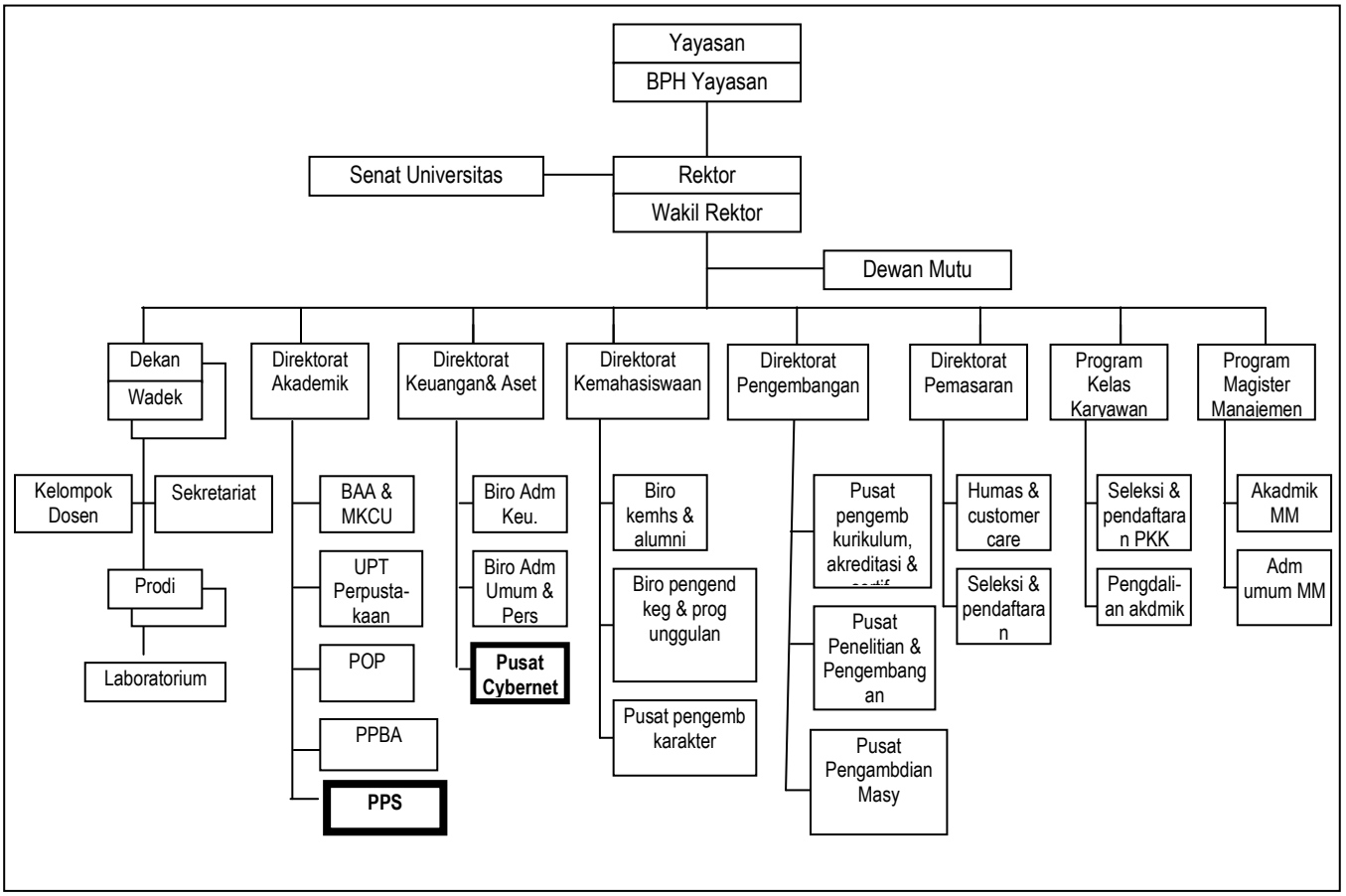
Kajian akan dilakukan dengan menggunakan panduan yang ada dalam melakukan sebuah kajian teknologi informasi/*IT assurance guide.* Kajian ini meliputi *detailed control objective* yang disesuaikan dengan keadaan dari Universitas XYZ (berdasar pada *high level control objective*). Kajian akan dilakukan dengan pendekatan audit yang sudah dibuat. Setelah proses pengkajian selesai tahap berikutnya adalah mendokumentasikan temuan-temuan hasil audit.

d. Melakukan analisa hasil audit

Setelah kajian dilakukan, selanjutnya menganalisis temuan-temuan yang didapat. Diharapkan hasil dari tahap analisis ini mendapatkan suatu kesimpulan alasan terjadinya permasalahan serta solusi terhadap permasalahan tersebut.

3. Audit Dengan Kerangka Kerja *IT Assurance Guide*

Pada bagian ini akan dipaparkan tentang penggunaan kerangka kerja *IT Assurance* yang digunakan dalam melakukan audit TI di Universitas XYZ. Sebelumnya akan dijelaskan alasan penggunaan *control objective* dari COBIT dibandingkan dengan yang lain seperti Ron Weber [1], QAO, dan Jack Champlain [3].



Gambar 1. Struktur Organisasi Universitas XYZ saat ini.

3.1. *IT Assurance Guide* dengan Menggunakan COBIT versi 4.1

Sebelum melakukan pemilihan kerangka kerja audit yang akan digunakan, terlebih dahulu dilakukan perbandingan kelengkapan kontrol yang ada pada masing-masing kerangka kerja audit. Perbandingan itu ditujukan untuk mendapatkan sebuah gambaran lengkap dari kontrol yang ada pada setiap kerangka kerja audit dengan cara memetakan setiap kontrol proses yang ada pada setiap kerangka kerja.

Pemetaan yang dilakukan adalah pemetaan antara COBIT, Ron Weber, QAO dan Champlain dan pemetaan antara COBIT dan ITIL. Dari kedua pemetaan tersebut terlihat jelas bahwa kerangka kerja audit yang diajukan oleh COBIT lebih lengkap dalam melihat proses-proses yang ada dalam manajemen TI. Walaupun memang dari setiap kerangka kerja terdapat keunggulan masing-masing.

Untuk ITIL sendiri berdasarkan pemetaan yang ada, proses yang memiliki banyak kesamaan dengan kerangka kerja COBIT adalah pada domain *Delivery and Support*. Hampir semua proses dalam domain ini dapat dipetakan dalam ITIL.

3.2. Profil Universitas XYZ

Untuk dapat menggambarkan Universitas XYZ secara menyeluruh dan objektif, dicoba untuk melihat dari dua sisi profil universitas, yaitu dari sisi profil umum dan profil TI.

3.3. Profil Umum Universitas XYZ

Universitas XYZ terbagi menjadi tiga lokasi kampus, di kota Jakarta. Dalam penyelenggaraan proses pendidikan, universitas ini membagi menjadi dua kategori program, yaitu program reguler dan program kelas karyawan. Untuk penyelenggaraan jenjang pendidikan S1 dan D3, terdapat 7 fakultas dan 21 program studi sedangkan untuk jenjang pendidikan S2 terdapat 4 program studi. Jumlah mahasiswa yang menuntut ilmu di Universitas XYZ sampai dengan tahun akademik 2007/2008 adalah sebanyak 11.000 mahasiswa (sumber: wawancara dengan direktur akademik,07). Dengan lebih dari 200 karyawan tetap dan karyawan kontrak, serta 130 lebih dosen tetap dan 170 lebih dosen tidak tetap, universitas XYZ termasuk universitas swasta terbesar di Jakarta. Untuk struktur organisasi Universitas XYZ dapat dilihat pada Gambar 1. Dari struktur organisasi tersebut terlihat bahwa sebenarnya unit TI

sendiri belum berada langsung dibawah Rektor. Unit ini secara formal terpecah menjadi 2 bagian, yaitu bagian pengembangan sistem dan bagian Cybernet. Keduanya berada dibawah dua direktorat yang berbeda. Pusat Pengembangan Sistem berada dibawah direktorat Akademik, sedangkan untuk bagian Cybernet terdapat pada direktorat Keuangan dan Pengelolaan Aset.

3.4. Profil Teknologi Informasi di Universitas XYZ

Sifat penggunaan TI di Universitas XYZ masih berada dalam tahap pendukung atau *support*, karena apabila tidak ada dukungan TI pun, *core* bisnis dari Universitas ini masih dapat berjalan. Profil TI di Universitas XYZ bisa dikatakan pada taraf yang cukup, hal ini dapat dilihat dari pengukuran tingkat kematangan pemanfaatan TI sekitar 43%, yang juga dilakukan dengan kerangka kerja COBIT.

Seperti yang telah disebutkan sebelumnya bahwa di Universitas XYZ, secara formal memang belum terbentuk sebuah unit TI, tetapi ada dua unit yang sudah melakukan kegiatan yang mirip ke arah manajemen TI. Unit tersebut adalah PPS (Pusat Pengembangan Sistem) dan unit Cybernet. Kedua unit pun tidak berada dalam satu direktorat yang sama. PPS yang berada langsung dibawah direktorat akademik merupakan penunjang direktorat akademik itu sendiri, dengan alasan karena *core* dari bisnis adalah akademik, maka para pengambil keputusan lebih menitikberatkan pengembangan sistem yang mendahulukan kepentingan akademik, itulah sebabnya mengapa PPS berada di bawah direktorat akademik.

Tabel 1. Daftar Aplikasi pada Universitas XYZ

NO	NAMA APLIKASI	FUNGSI	STATUS	LOKASI IMPLEMENTASI	PENGGUNA
1.	Aplikasi Sistem Informasi Akademik	Aplikasi SIAK sebagai penunjang aktivitas perkuliahan di Universitas XYZ	Sudah berjalan	Universitas XYZ	Civitas Akademika Universitas XYZ
2.	Aplikasi Online Perpustakaan	Aplikasi yang mengelola otomasi perpustakaan	Sudah berjalan dan sedang dalam tahap upgrading	UPT Perpustakaan	Civitas Akademika Universitas XYZ
3.	Aplikasi Sistem Wisuda	Aplikasi pengelolaan data pendaftaran wisuda	Sudah berjalan	Biro Administrasi Akademik	Biro Administrasi Akademik
4.	Aplikasi PPMB	Aplikasi pengelolaan data pendaftaran calon mahasiswa	Sudah berjalan	Pemasaran dan Biro Administrasi Akademik	Pemasaran dan Biro Administrasi Akademik
5.	Aplikasi Pembayaran Honor Dosen	Aplikasi untuk mengelola manajemen pembayaran honor dosen	Sudah berjalan	Biro Administrasi Keuangan	Biro Administrasi keuangan
6.	Sistem Penggajian Karyawan	Digunakan untuk penggajian karyawan (masih menggunakan MS.Excel)	Sudah berjalan	Biro Administrasi Keuangan	Biro Adminkistrasi keuangan
7.	Aplikasi Sistem Logistik	Digunakan sebagai penunjang sistem logistik	Sudah berjalan	Unit Logistik	Biro Administrasi Umum
8.	Portal Universitas XYZ (WEB)	Aplikasi wb internet yang menggambarkan aktivitas Univeritas keseluruhan	Sudah berjalan	Seluruh jaringan WAN	Civitas Akademika dan publik
9.	Aplikasi Universitas XYZ Karir	Aplikasi untuk mendata dan membantu mahasiswa dan alumni (khususnya) dalam mencari pekerjaan	Sudah berjalan	Seluruh jaringan WAN	Civitas Akademika, coorporate, dan publik
10.	Aplikasi Sistem Inventaris	Aplikasi ini untuk mendata pengelolaan data barang dan penomeran barang	Sudah berjalan	Unit inventaris	Biro Administrasi Umum

Tabel 2. Daftar tabel dalam SIAK

No	Nama Tabel
1	Data Tabel Fakultas
2	Data Tabel Jurusan
3	Data Tabel Gedung
4	Data Tabel Ruangan
5	Data Tabel Propinsi
6	Data Tabel Jabatan
7	Data Tabel Dosen
8	Data Tabel Biaya Per-angkatan
9	Data Tabel Rekening Bank
10	Data Tabel Jenis Mata Kuliah
11	Data Tabel Mata Kuliah
12	Data Tabel Literatur
13	Data Tabel Mahasiswa
14	Data Tabel Prosentase Nilai
15	Data Tabel Range Nilai Matakuliah

Walaupun demikian PPS tidak akan menutup kemungkinan untuk melakukan pengembangan sistem bagi seluruh unit kerja lain yang ada di Univeritas XYZ. Sementara unit yang lain, yaitu Cybernet berada di bawah direktorat keuangan dan pengelolaan aset, karena unit ini hanya sebagai *implementor* atau pendukung dari kegiatan bisnis Universitas yang berkaitan dengan TI. Hal ini disimpulkan bahwa Cybernet berurusan dengan aset TI yang ada seperti komputer, jaringan, perangkat lunak atau sistem dan perangkat keras lainnya.

Untuk melakukan koordinasi antara PPS dan Cybernet masing-masing ada *work instruction* yang dibuat di masing-masing unit (hal ini ada karena Universitas ini sudah menerapkan ISO 9001 untuk manajemen pelayanan).

3.5. Rencana Strategis TI

Saat ini Universitas XYZ sudah memiliki Rencana Strategis TI, walaupun masih dirasa kurang tetapi sudah cukup menguraikan strategi tingkat tinggi kemana pengembangan TI akan diarahkan. Berdasarkan dokumen Rencana Strategis TI terdapat 8 area strategis pengembangan TI, yaitu:

1. Akademik
2. Pengelolaan fasilitas/aset
3. Sumber Daya Manusia
4. Logistik
5. Alumni
6. Pemasaran/Humas
7. *Auxillary Business*
8. Keuangan

Dikarenakan *core* bisnis dari Universitas adalah pelayanan pendidikan maka yang akan dikembangkan terlebih dahulu adalah sistem akademik.

3.6. Infrastruktur TI

Secara fisik infrastruktur TI di kampus terutama di Universitas XYZ merupakan infrastruktur jaringan komputer yang terdiri dari tujuh *core* kabel serat optik *multi-mode* yang menghubungkan tujuh *high-speed switch* yang tersebar di seluruh ruang kantor dan laboratorium. Untuk menghubungkan antara satu kampus dengan kampus lainnya, digunakan jalur umum (*public network*) melalui VPN. Untuk jaringan komputer di dua kampus lainnya hanya menggunakan kabel UTP dengan kecepatan 100Mbps. Universitas XYZ memiliki ruang *server* utama yang berisi *web server*, mail *server*, *proxy server*, dan beberapa *backup server*. Teknologi prosesor *server-server* ini setara dengan Pentium 4 pada kisaran 1,7 – 2,6 MHz. Setiap laboratorium komputer terhubung ke *server-server* ini sehingga mahasiswa dapat mengisi kartu rencana studi (KRS), melihat nilai, dan sebagainya dari laboratorium di program studi masing-masing. Hal ini bahkan dapat dilakukan dari rumah, khusus untuk kelas karyawan.

Selain infrastruktur kabel, juga terdapat infrastruktur jaringan nirkabel (WLAN) yang dapat di akses secara bebas oleh mahasiswa di Kampus utama dan kedua kampus lainnya. Secara logis jaringan komputer dibagi menjadi *subnet-subnet*. Dengan demikian di sini diterapkan teknologi WAN seperti *routing*, DNS, dan sebagainya.

3.7. Aplikasi yang Ada

Dari sisi perangkat lunak, khususnya untuk laboratorium dan komputer *client*, infrastruktur telah menggunakan sistem operasi dari Microsoft di bawah lisensi *Microsoft Campus Agreement*. Untuk s*erver*, lebih banyak menggunakan Linux. Terdapat 10 jenis aplikasi yang ada dan baru akan dijalankan di Universitas XYZ, dimana kesemuanya belum terintegrasi satu dengan yang lain. Tabel 1 memperlihatkan daftar aplikasi apa saja yang ada.

3.8. Basis Data dalam SIAK Universitas XYZ

Pada Sistem Informasi Akademik di Universitas XYZ, basis data yang digunakan adalah basis data dengan model relasional. DBMS yang digunakan adalah Oracle 9i Enterprise Edition. Tabel yang ada pada SIAK Universitas XYZ ada 15 tabel, dapat dilihat pada Tabel 2 dibawah ini. Untuk sebagian tabel yang digunakan dalam SIAK sudah terintegrasi atau digunakan untuk aplikasi yang lain. Contohnya aplikasi PPMB (Pendaftaran dan Pengelolaan Mahasiswa Baru). Adapun untuk perancangan basis data dalam SIAK memang tidak melalui tahapan perancangan basis data pada umumnya, karena memang tidak melalui tahap analisis dan perancangan tetapi lebih kepada pemenuhan tabel-

tabel yang harus ada untuk menyimpan data dalam program-program yang dibuat.

4. *IT Assurance* Di Universitas XYZ

Seperti yang telah disebutkan sebelumnya bahwa dalam kerangka kerja *IT Assurance* yang diusulkan oleh COBIT terdapat tiga tahapan besar yang mesti dijalani dalam audit TI. Dari tahapan ini masih terdapat sub tahapan lagi. Dalam melakukan audit, tidak mengikuti semua sub tahapan yang ada pada publikasi *IT Assurance guide*, karena sub tahapan yang ada bersifat redundan, sehingga dicoba meringkas (*summarize*) tahapan tersebut menjadi:

1. Tahap perencanaan
   a) Dasar audit.
   b) Kerangka kerja audit TI yang digunakan.
   c) Analisa awal terhadap resiko.
2. Tahap pembatasan lingkup kajian
   a) Tujuan dari dilakukannya audit.
   b) Pendokumentasian arsitektur TI Universitas XYZ.
   c) Pemilihan kontrol kerangka kerja yang dijalankan oleh unit TI Universitas XYZ.
   d) Mengidentifikasi proses TI yang akan dikaji.
   e) Melakukan seleksi terhadap komponen TI di Universitas XYZ.
3. Tahap pelaksanaan
   a) Melakukan pengujian terhadap kontrol yang sudah ditetapkan.
   b) Melakukan pengujian hasil *control objective.*
   c) Mendokumentasikan akibat dari kelemahan kontrol.
   d) Menyimpulkan laporan dan memberikan rekomendasi.

4.1. Tahap Perencanaan

4.1.1. Dasar Audit

Audit TI yang dilakukan di Universitas XYZ atas dasar penelitian untuk laporan evaluasi manajemen TI di Universitas XYZ.

4.1.2. Kerangka kerja audit

Kerangka kerja audit yang digunakan adalah COBIT. Dengan menggunakan 34 *control objective* yang dibahas lagi lebih detil dalam 210 *detailed control objective*.

4.1.3. Analisis Resiko

Pada analisis resiko dicoba mengikuti beberapa panduan dari *IT Assurance guide: using COBIT* [5]. Analisis resiko dari Universitas XYZ dibagi kedalam penentuan aset yang harus dilindungi, ancaman dan resiko yang terjadi bila aset tersebut tidak memiliki kontrol yang layak. Dalam mengidentifikasi aset, dikategorisasikannya menjadi:

1. Rencana Strategis Sistem Informasi
2. Struktur organisasi
3. Sumber daya manusia pada unit cyber
4. Sumber daya manusia pada Pusat Pengembangan Sistem
5. *Software* aplikasi
6. *Password management*
7. Prosedur penggunaan aplikasi
8. Basis data
9. Portal organisasi
10. Jaringan komputer
11. Pelayanan kepada *user*

4.2. Tahap Pembatasan lingkup *IT Assurance*

4.2.1. Tujuan

Tujuan dari dilakukannya audit TI adalah untuk mengevaluasi sejauh mana manajemen TI di Universitas XYZ diterapkan, selain itu juga hasil temuan dan rekomendasi perbaikan dan pengembangan sistem TI yang ada saat ini.

4.2.2. Penyeleksian *Control Objective*

Control objective yang digunakan adalah *detailed control objective* dari 34 *control objective* yang ada pada COBIT sebanyak 210 *detailed control objective*.

4.2.3. Mendokumentasikan arsitektur yang ada di Universitas XYZ.

Hal ini dilakukan dengan cara wawancara dengan personil utama dari Univeritas XYZ, yaitu Kepala Pusat Pengembangan Sistem, Kepala Cybernet dan beberapa staf TI yang ada di unit Cybernet.

4.2.4. Mengidentifikasi Proses yang Akan Dikaji

Dalam kajian ini audit TI akan melingkupi semua domain yang ada, yaitu *plan and organise, acquire and implementation, delivery and support* dan *monitor and evaluation.*

4.2.5. Mengidentifikasi Komponen TI Universitas XYZ

Komponen yang akan dikaji hanya aplikasi SIAK Universitas XYZ, basis data yang ada, infrastruktur jaringan yang ada di kampus utama dan orang-orang yang ada di kedua unit TI (PPS dan Cybernet).

4.3. Tahap Pelaksanaan

Dari daftar *control objective* yang ada di Universitas XYZ, penulis mengembangkan lebih lanjut ke tahap pelaksanaan yang berikutnya yaitu:

1. Tahap pengujian kelengkapan kontrol
   Tahap pengujian kontrol yang dilakukan adalah dengan mengidentifikasi kelengkapan *control objective* dan keefektifan dari *control objective* dalam proses-proses TI di Univerisitas XYZ. Berdasarkan hasil pengujian dari 34 *control objective* yang ada hampir 85% tidak memiliki kontrol yang lengkap.
2. Tahap berikutnya adalah tahap pengujian terhadap hasil *control objective.*
   Pada tahap ini yang akan diuji adalah hasil dari adanya *control objective* yang efektif di universitas XYZ. Hasilnya adalah mendekati kisaran 30% efektif berdasarkan dari kontrol yang ada / memadai.

4.4. Temuan Hasil Audit

Dari kajian yang dilakukan terhadap kondisi TI yang ada di Universitas XYZ, didapatkan temuan-temuan yang berhubungan dengan lemahnya kontrol yang diterapkan. Temuan-temuan hasil audit yang dilaporkan meliputi:

i. Rencana dan Strategi TI universitas XYZ
ii. Keorganisasian pengelolaan TI
iii. SIAK Universitas XYZ
iv. Perancangan aplikasi dan basisdata
v. Pengembangan dan pengubahan aplikasi
vi. Pengelolaan basisdata
vii. Jaringan komputer yang ada dikampus utama Universitas XYZ
viii. Layanan ke pengguna
ix. Portal organisasi.

4.4.1. Rencana dan Strategi TI Universitas XYZ

1. Universitas XYZ sudah mempunyai konsep Rencana Strategis Teknologi Informasi namun belum cukup sempurna sehingga sampai dengan audit TI yang dilakukan, Rencana Strategis TI belum dijadikan sebagai acuan dari setiap pengembangan sistem yang ada (sistem yang dibangun bersifat *adhoc*).
2. Dalam melakukan pemilihan arsitektur basis data, arsitektur jaringan dan aplikasi yang akan dikembangkan, Universitas XYZ tidak melakukan studi formal, misalkan dengan melakukan tahap *cost benefit analysis*, atau *risk analysis*.

4.4.2. Keorganisasian Pengelolaan TI

1. Struktur organisasi TI
   Struktur organisasi TI yang ada di Universitas TI terbagi menjadi dua unit dan dibawah dua direktorat yang berbeda, hal ini dapat menyebabkan:
   a. Pengurangan tingkat independensi pengelolaan TI karena tidak dibawah satu direktorat TI sendiri yang bertanggung jawab langsung kepada rektor
   b. Terpisahnya antara pusat pengembangan sistem sebagai pihak perencana dan Cybernet sebagai pihak operasional akan menyulitkan kontrol terhadap komunikasi antar dua belah pihak.
2. Staf TI
   a. Untuk unit Cybernet yang sudah ada terlebih dahulu masih belum cukup dalam jumlah staf TI, dalam hal ini dibutuhkan staf yang dapat membantu untuk menjalankan peran pemeliharaan dan operasional seperti *IT service desk*, *IT support*, *desktop support*.
   b. Untuk unit Pusat Pengembangan Sistem perlu dibutuhkan staf ahli dalam perencanaan dan pengembangan sistem seperti *database administrator*, *programmer aplikasi*, *system analyst*, *tester engineer*.

4.4.3. SIAK Universitas XYZ

1. *User account management*
   SIAK sudah memiliki fitur untuk mengingat *password* tanpa harus tergantung pada staf unit Cybernet tetapi belum berjalan dengan yang diharapkan, pengguna masih bertanya kepada staf Cybernet perihal lupa *password*.
2. Penggunaan
   a. SIAK belum memiliki bantuan asistensi penggunaan aplikasi dalam bentuk menu standar *help*
   b. Dikarenakan pengembangan SIAK tidak mengikuti fase-fase pengembangan proyek seperti *user requirement*, maka dirasa masih banyak kekurangan atau ketidaksesuaian yang dirasa oleh *user*.
3. Proses kerja
   Untuk pengisian nilai yang dimulai dari periode UTS, SIAK belum dapat menampilkan data kelas dan mahasiswa yang *up to date*.

4.4.4. Perancangan Aplikasi dan Basisdata

1. Untuk perancangan basis data tidak megikuti kaidah-kaidah perancangan yang umum, sehingga tidak terdapat dokumentasi yang lengkap mengenai hal tersebut.
2. Tidak terdapat diagram relasi untuk basis data sehingga basis data yang ada tidak didasari pada pendekatan analisis.

4.4.5. Pengembangan dan Perubahan Aplikasi

Pada awal pengembangan aplikasi SIAK tidak memiliki dokumentasi formal sehingga apabila

programmer yang bersangkutan berhalangan atau berhenti maka tidak bisa dilakukan pengembangan terhadap SIAK, kecuali pembuatan dari awal kembali.

4.4.6. Pengelolaan Basisdata

1. Fungsi *audit trail* pada *database server* belum diaktifkan. Hal tersebut menimbulkan kesulitan untuk mengetahui dan menyelidiki insiden yang terjadi pada *database server.*
2. Proses *backup* dilakukan setiap tujuh hari sekali, hal tersebut menimbulkan resiko gangguan, kerusakan dan kehilangan data pada saat setelah proses *backup* terakhir kali dilakukan sampai proses *backup* berikutnya.

4.4.7. Jaringan Komputer Kampus Utama Universitas XYZ

1. Pembagian *network* di Universitas XYZ tidak berdasarkan pada fungsi yang sama, tetapi berdasarkan lokasi tempat *device* berada. Sehingga akan menyulitkan bagi satu unit yang sama tetapi menempati gedung yang berlainan untuk dapat membagi data.
2. *Security* masih dilakukan di tingkat jaringan saja misalkan dengan *firewall* atau *Intrussion Detection System*, dan kurang memperhatikan keamanan fisik, hal ini dilihat dari pengamanan yang kurang terhadap *switch-switch* yang ada pada setiap *network*.

4.4.8. Layanan ke Pengguna

1. Sebagian besar komputer yang ada di lingkungan kampus utama, tidak dilengkapi dengan *software antivirus* yang berlisensi maupun gratis (hanya pada komputer-komputer tertentu saja seperti di laboratorium komputer). Walaupun ada *software* tetapi tidak ter-*update* secara rutin.
2. Universitas XYZ belum memiliki kebijakan dan prosedur untuk mendeteksi, melaporkan dan merespon atas terjadinya insiden terhadap keamanan komputer.

4.4.9. Portal Organisasi

Terdapat keterlambatan *updating* isi situs web dari Univeritas XYZ, sehingga terkesan berita-berita seputar civitas akademika tidak dinamis.

4.5. Rekomendasi

Rekomendasi yang disampaikan merupakan hasil analisis terhadap temuan-temuan yang didapat dari pengujian keefektifan kontrol dan hasil pengujian terhadap *output* kontrol.

Dalam memberikan rekomendasi, dibagi menjadi tiga jangka waktu pencapaian, yaitu rekomendasi jangka pendek yang berkaitan dengan hal-hal yang harus dengan segera dilakukan oleh Universitas XYZ agar proses-proses TI yang ada masih tetap berjalan dengan baik. Untuk rekomendasi jangka menengah, dilakukan pengklasifikasian berdasarkan perencanaan strategis di unit TI, sementara untuk rekomendasi jangka panjang diberikan rekomendasi yang berkenaan dengan kebijakan Universitas setingkat dengan kebijakan organisasinya.

4.5.1. Rekomendasi Jangka Pendek

1. Agar Universitas XYZ meminta unit Cyber untuk menyempurnakan fitur untuk:
   a. Mensosialisasikan cara untuk mengingat *password* dengan cara mandiri tanpa harus melalui bantuan staf unit Cybernet.
   b. Memaksa *user* untuk selalu mengganti *password* secara berkala.
   c. Mencegah usaha *login* coba-coba yang dilakukan secara berturut-turut.
   d. Merekam usaha *login* yang tidak berhasil.
   e. Merekam setiap transaksi yang dilakukan oleh pengguna.
   f. Menambah fasilitas *help* yang akan mempermudah dalam penggunaan aplikasi SIAK.
   g. Memperbaiki skema basisdata
   h. Melakukan *backup* dengan kondisi:
      - Frekuensi pembuatan *backup* lebih sering.
      - *Backup* dilakukan terhadap data *audit trail* (*log*) DBMS
   i. Membuat rencana tertulis yang menjelaskan secara lengkap rencana perubahan/ modifikasi/*upgrade* aplikasi SIAK.
   j. Menyediakan *antivirus* pada setiap komputer dan melakukan *update* rutin dari *server*.
   k. Menyelesaikan masalah-masalah penggunaan aplikasi SIAK kepada semua *user* melalui penyediaan manual penggunaan aplikasi, asistensi langsung secara proaktif.
   l. Merancangan arsitektur jaringan di Universitas XYZ berdasarkan pada fungsi unit bukan berdasarkan lokasi *device* dengan menggunkan VLAN.
   m. Mengatur *security* jaringan di tingkat fisik dengan cara menempatkan *switch*/*router* pada tempat tersendiri dan diberi pengaman yang memadai seperti kunci sendiri kedalam ruangan tersebut.
2. Agar Universitas XYZ melakukan usaha-usaha untuk menyediakan tenaga staf yang kompeten untuk posisi minimal:

a. *Database administrator* yang bertanggungjawab untuk melakukan pengelolaan basis data.
b. *IT service desk* yang bertanggungjawab untuk mengelola keluhan pengguna yang berhubungan dengan penggunaan teknologi informasi.
c. *IT support* yang bertanggungjawab untuk menyelesaikan masalah-masalah yang berhubungan dengan *hardware* dan jaringan komputer yang dialami oleh pengguna.
d. *Tester engineer* yang bertanggungjawab untuk mengelola *testing* atas aplikasi sistem informasi.

3. Agar Universitas XYZ secara bertahap melaksanakan pengembangan dan implementasi kebijakan, prosedur dan proses kerja yang terkait dengan:
   a. Identity management
   b. User account management
   c. Backup, storage and retention management
   d. Service desk and incident management
   e. Problem management
   f. Change management
   g. IT supplier management
   h. IT security management

4.5.2. Rekomendasi Jangka Menengah

1. Agar Universitas XYZ melakukan pengembangan atau penyempurnaan dan pemberlakuan perencanaan strategis TI yang meliputi:
   a. IT Strategic Plan
   b. IT Tactical Plan
   c. IT Portfolio Management
2. Agar Universitas XYZ melakukan pengembangan dan pemberlakuan arah teknologi Universitas XYZ yang meliputi:
   a. Technological Direction Plan
   b. Technological Infrastructure Plan
3. Agar Universitas XYZ melakukan pengembangan dan pemberlakuan arsitektur informasi organisasi Universitas yang meliputi:
   a. Enterprise Information Architecture Model
   b. Enterprises Data Dictionary and Data Syntax Rules
   c. Data Classification Scheme
4. Agar Universitas XYZ melakukan usaha-usaha untuk merealisasikan unit Cybernet dan PPS dalam sebuah unit TI yang berada pada satu direktorat yang sama.

4.5.3. Rekomendasi Jangka Panjang

Agar Universitas XYZ dapat menyempurnakan struktur organisasinya dalam hal yang terkait dengan pengelolaan TI, yaitu:

a. Menyusun sebuah direktorat khusus untuk perencanaan, pengembangan, dan pengelolaan TI yang bertanggung jawab penuh kepada rektor.
b. Menyusun sebuah direktorat yang membawahi kepala pusat perencanaan, pengembangan dan pemerliharaan TI.

1. Agar Universitas XYZ melakukan usaha-usaha untuk menyediakan atau melengkapi tenaga personal yang kompeten untuk rekomendasi butir 1 diatas.
2. Agar Unversitas XYZ melakukan pengelolaan TI yang baik dan sehat (*Good IT Governance*) melalui peningkatan tingkat kematangan dan kefektifan kontrol pada proses TI sesuai dengan kerangka kerja yang digunakan, dalam hal ini adalah COBIT. Skala prioritas pelaksanaannya dapat mempertimbangkan faktor kebutuhan, analisa *cost & benefit*, resiko serta faktor lainnya. Mengenai urutan prioritas, dapat disesuaikan dengan kondisi pada saat itu.

5. Kesimpulan

Dari pembahasan sebelumnya, dapat menarik kesimpulan sebagai berikut:

1. Dari hasil pengujian terhadap keefektifan kontrol sudah ada kontrol yang berjalan yaitu PO8.1. *Quality Management System*, PO8.4. *Customer Focus*, PO8.5 *Continuous Improvement* dan PO8.6 *Quality Measurement, Monitoring and Review*, hal itupun karena ada penerapan standarisasi ISO. Kontrol yang lainnya adalah DS5.9. *Malicious Software Prevention, Detection and Correction.*
2. Masih ada proses TI yang belum memiliki kontrol sama sekali seperti yang didefinisikan oleh COBIT, yaitu:
   a. Domain Plan and Organise
   PO3 Determine Technological Direction
   PO5 Manage the IT Investment
   PO9 Assess and Manage IT Risks
   PO10 Manage Projects
   b. Domain Acquire and Implementation
   AI1 Identify Automated Solution
   AI7 Install and Accredit Solutions and Changes
   c. Domain Delivery and Support
   DS3 Manage Performance and Capacity
   DS4 Ensure Continuous Service
   DS6 Identify and Allocate Cost
   DS10 Manage Problem
   DS11 Manage Data
   DS12 Manage the Physical Environment

d. Domain Monitor and Evaluate

ME1 Monitor and Evaluate IT performance
ME2 Monitor and Evaluate Internal Control
ME3 Ensure Regulatory Compliance
ME4 Provide IT Governance

Sisa dari kontrol yang ada sudah terdapat kontrol yang sesuai dengan kerangka kerja COBIT namun masih belum memadai.

3. Di Universitas XYZ tidak ada mekanisme pemantauan dan pengevaluasian kinerja yang dilakukan di kedua unit TI (PPS dan Cybernet) hal ini terbukti dari kontrol yang ada pada domain *Monitor* dan *Evaluate* yang masih tidak ada sama sekali.
4. Berdasarkan temuan-temuan yang ada, dapat disimpulkan bahwa manajemen TI yang kurang memadai dikarenakan kurangnya sumber daya manusia yang mengelola.

REFERENSI

[1] Weber, Ron *Information system Control Audit* New Jersey: Prentice Hall, 1999.
[2] *IT Governance Institute*. COBIT 4.0: Chicago, 2007.
[3] Champlain, Jack J. *Auditing Information System: A Comprehensive Reference Guide* New York: John Wiley & Son, 1998.
[4] "*ITIL-The Key to Managing IT Services version 2.1*", 2002, TSO-OGC [CD-ROM].
[5] *IT Assurance Guide: Using COBIT,* Chicago, 2007.