LAMPIRAN A
MODEL STANDAR TATA KELOLA TI

A.1 Standar COSO, ISO/IEC 17799 dan ITIL

A.1.1 COSO

COSO merupakan kependekan dari *Committee of Sponsoring Organization of the Treadway Commission*, sebuah organisasi di Amerika Serikat yang berdedikasi dalam meningkatkan kualitas pelaporan finansial yang mencakup etika bisnis, kontrol internal, dan *corporate governance*. Komisi ini didirikan pada tahun 1985 untuk mempelajari faktor-faktor yang menunjukkan ketidaksesuaian dalam pelaporan finansial.

Pada awal tahun 90-an, *Pricewaterhouse Couper* bersama komisi ini melakukan *extensive study* mengenai kendali internal, yang menghasilkan kerangka kerja COSO. Sejak saat itu, komunitas finansial global termasuk badan-badan regulator seperti *public accounting* dan *internal audit professions* telah mengadopsi COSO.

Kerangka kerja COSO terdiri dari tiga dimensi, yaitu:

1. Komponen Kendali (*Component control*). Dimensi ini terdiri atas 5 komponen kendali internal yang diintegrasikan dan dijalankan dalam semua unit bisnis, dan akan membantu mencapai sasaran kendali internal, yang meliputi:
   a. *Monitoring*. Mencakup proses pengukuran kinerja sistem kendali yang diterapkan, aktifitas-aktifitas pengelolaan dan pengawasan, dan kegiatan audit internal.
   b. *Information and communication*. Mencakup akses informasi internal dan eksternal, serta alur informasi dalam perusahaan.
   c. *Control activities*. Kebijakan atau prosedur yang berisi arahan manajemen yang harus diikuti oleh setiap pihak terkait.
   d. *Risk assesment*. Identifikasi resiko yang dijadikan dasar untuk menentukan aktifitas-aktifitas kendali yang akan diterapkan.
   e. *Control environment*. Merupakan taraf kendali perusahaan dimana kendali internal dikembangkan secara *top-down*.

2. Sasaran Kendali Internal (*Internal control objectives*). Merupakan tujuan yang akan dicapai dari setiap kendali internal. *Internal control objectives* dikategorikan ke dalam 3 area, yaitu:
   a. *Operation*. Efektifitas dan efisiensi operasi untuk mencapai tujuan bisnis.
   b. *Financial*. Kehandalan dan pertanggungjawaban laporan keuangan yang dipublikasikan.
   c. *Compliance*. Pemenuhan terhadap hukum dan peraturan yang berlaku.

3. Unit/Aktifitas Organisasi (*Unit / activities of an organization*). Dimensi ini mengidentifikasi unit-unit atau aktifitas-aktifitas di dalam perusahaan yang memerlukan kendali internal. Kendali internal menyangkut keseluruhan organisasi dan semua bagian-bagiannya.

A.1.2 ISO/IEC 17799

ISO/IEC 17799 adalah kode praktis pengelolaan keamanan informasi yang dikembangkan oleh *The International Organization for Standardization* (ISO) dan *The International Electrotechnical Commission* (IEC). ISO/IEC 17799 adalah panduan yang terdiri dari saran dan rekomendasi yang digunakan untuk memastikan keamanan informasi perusahaan.

ISO/IEC 17799 bertujuan memperkuat tiga elemen dasar keamanan informasi, yaitu:

a. *Confidentiality*. Memastikan informasi hanya dapat diakses oleh pihak-pihak yang berwenang atau memiliki otoritas.
b. *Integrity*. Menjaga akurasi dan kelengkapan informasi ketika diproses.
c. *Availability*. Memastikan bahwa pihak-pihak yang memiliki otoritas dapat mengakses informasi dan aset-aset terkait lainnya ketika diperlukan.

ISO/IEC 17799 disajikan dalam bentuk panduan dan rekomendasi yang terdiri dari 36 *security objectives* dan 127 *security controls* yang dikelompokkan ke dalam 10 domain keamanan informasi. Berikut ini 10 domain keamanan informasi ISO/IEC 17799:

a. *Security policy*. Menyajikan panduan dan arahan bagi manajemen dalam meningkatkan keamanan informasi.
b. *Organizational security*. Memfasilitasi pengelolaan keamanan informasi dalam perusahaan.
c. *Asset classification and control*. Melakukan inventarisasi aset dan melindungi aset tersebut dengan efektif.
d. *Personel security*. Meminimalkan resiko yan disebabkan oleh kesalahan manusia, pencurian, dan penggunaan peralatan yang tidak benar.
e. *Physical and environmental security*. Mencegah tindakan kekerasan dan perusakan terhadap fasilitas dan data perusahaan.
f. *Communications and operations management*. Memastikan operasi yang dilakukan telah sesuai dengan kebutuhan bisnis dan peralatan yang digunakan dalam pemrosesan informasi tersebut dapat diandalkan.
g. *Access control*. Kendali-kendali yang diterapkan pada proses pengaksesan data atau informasi perusahaan.
h. *Systems development and maintenance*. Memastikan bahwa aspek keamanan informasi disertakan dalam proses pengembangan dan perawatan sistem informasi.
i. *Business continuity management*. Meminimalkan dampak dari terhentinya proses bisnis dan melindungi proses-proses penting perusahaan dari kegagalan dan kerusakan yang diakibatkan oleh ancaman keamanan informasi.
j. *Compliance*. Menghindarkan terjadinya tindakan pelanggaran dan memastikan ketaatan terhadap hukum maupun kesepakatan kontrak.

A.1.3 ITIL (*The Information Technology Infrastructure Library*)

ITIL dikembangkan oleh *The Office of Government Commerce* (OGC), suatu badan di bawah pemerintah Inggris melalui kerja sama dengan *The IT Service Management Forum* (ITSMF) yaitu suatu organisasi independen mengenai manajemen pelayanan TI dan *British Standard Institute* (BSI) yang merupakan badan penetapan standar pemerintah Inggris. ITIL merupakan sebuah kerangka kerja pengelolaan layanan TI, kumpulan *best practice* penerapan pengelolaan layanan TI. ITIL memberikan rekomendasi dan arahan yang dibutuhkan manajemen untuk mengelola layanan TI dalam perusahaan.

Pengelolaan layanan TI difokuskan pada 3 tujuan utama, yaitu menyelaraskan layanan-layanan TI perusahaan dengan kebutuhan bisnis dan konsumen pada saat ini dan yang akan datang, meningkatkan kualitas layanan TI, dan dalam jangka panjang, pengelolaan layanan TI dapat digunakan untuk menekan biaya pengadaan layanan-layanan TI. Kerangka kerja (*framework*) ITIL terdiri dari dua bagian, yaitu:

1. Dukungan Layanan (*Service support*)
    a. *Incident management*. Mengembalikan layanan TI ke tingkat pengoperasian normal secepat mungkin dan menekan dampak negatif yang disebabkan oleh insiden yang terjadi pada aktifitas bisnis perusahaan, memastikan ketersediaan, dan menjaga kualitas layanan TI pada tingkat terbaik.
    b. *Problem management*. Menekan dampak negatif dari suatu kesalahan yang terjadi pada infrastruktur TI dan mencegah terulangnya kembali kesalahan tersebut.
    c. *Configuration management*. Mencatat, menghitung dan memeriksa catatan-catatan konfigurasi komponen-komponen infrastruktur TI perusahaan, dan memastikan seluruh proses pengelolaan informasi dapat berjalan dengan baik.
    d. *Change management*. Memastikan efektifitas dari metode dan prosedur standarisasi yang diterapkan dalam menangani seluruh perubahan dan menekan dampak yang diakibatkan oleh perubahan tersebut.

e. *Release management*. Memastikan komponen-komponen infrastruktur TI perusahaan (perangkat keras, perangkat lunak, *firmware*) yang digunakan dapat berjalan sesuai jadwal dan terbebas dari gangguan.

2. Penyampaian Layanan (*Service delivery*)

a. *Service level management*. Memastikan seluruh kesepakatan pemenuhan layanan TI (*service level agreement*) telah ditaati, dipenuhi dan dampak yang merugikan yang disebabkan oleh kualitas TI yang rendah dapat ditekan ke tingkat yang dapat diterima.

b. *Financial management for IT services*. Memastikan pengaturan biaya dan redistribusi biaya yang akurat untuk meningkatkan ketersediaan sumber daya keuangan.

c. *Capacity management*. Memastikan tingkat kelangsungan layanan dan pengelolaan sumber daya TI sesuai dengan kapasitas yang harus disediakan, mencakup *business capacity*, *service capacity*, dan *resource capacity*.

d. *IT Service continuity management*. Meminimumkan efek negatif yang disebabkan oleh bencana alam dan kejadian-kejadian yang tidak dapat diprediksi, gangguan terhadap proses bisnis dapat dikurangi.

e. *Availability management*. Pemantauan dan peningkatan yang terusmenerus terhadap ketersediaan sistem untuk memastikan konsistensi ketersediaan layanan TI yang dibutuhkan proses bisnis. Standar ITIL berfokus kepada proses layanan TI, dan sama sekali tidak menyertakan proses penyelarasan strategi perusahaan terhadap strategi TI yang dikembangkan.

LAMPIRAN B
CONTROL OBJECTIVES
DAN
RESIKO YANG DAPAT DIATASI

Nama Proses	Control Objectives	Resiko
PO10 Manage Projects	PO10.1 Programme Management Framework	• Inappropriate project prioritisation • Disorganised and ineffective approach to project programmes • Misalignment of project and programme objectives
	PO10.2 Project Management Framework	• Different project management approaches within the organization • Lack of compliance with the organization's reporting structure • Inconsistent tools for project management
	PO10.3 Project Management Approach	• Confusion and uncertainty caused by different project management approaches within the organisations • Lack of compliance with the organisation's reporting structure • Failure to respond to project issues with optimal and approved decisions
	PO10.4 Stakeholder Commitment	• Unclear responsibilities and accountabilities for ensuring cost control and project succes • Insufficient stakeholder participation in defining requirement and reviewing deliverables • Reduced understanding and delivery of business benefits
	PO10.5 Project Scope Statement	• Misunderstanding of project ojectives and requirement • Failure of projects to meet business and user rquirement • Misunderstanding of the impact of this project with oter related projects
	PO10.6 Project Phase	• Lack of alignment of projects to

	Initiation	the organisation's vision • Wrong prioritisation of projects • Undetected deviations from the overall project plan • Poor utilisation of resources
	PO10.7 Integrated Project Plan	• Undetected errors in project planning and budgeting • Lack of alignment of projects to the organisation'sobjective and to other interdependent projects • Undetected deviations from the project plan
	PO10.8 Project Resources	• Gaps in skill and resources jeopardising critical project tasks • Inefficient use of resources • Contract disputes with outsourced resources
	PO10.9 Project Risk Management	• Undetected project risks • Lack of mitigating actions for identified risks • Undetected project showstoppers
	PO10.10 Project Quality Plan	• Project deliverables failing to meet business and user requirements • Gaps in expected and delivered qualitywithin the projects • Inefficient and fragmented approach to quality assurance • Implemented system or changes adversely impact existing systems and infrastructures
	PO10.11 Project Change Control	• Lack of control over project scope, cost and schedue • Lost business focus • Inability to manage resources
	PO10.12 Project Planning of Assurance Methods	• Untrustworthly assurance activities • Ineffective and/or inefficient assurance activities

		• Accreditation and implementation delays
	PO10.13 Project Performance Measurement, Reporting and Monitoring	• Ineffective reporting on project progress and unidentified issues • Lack of control over project progress • Loss of focus on customer expectations and business needs
	PO10.14 Project Closure	• Undetected project management weaknesses • Mised opportunities from lessons learned

LAMPIRAN C
TRANSKRIP WAWANCARA

TRANSKRIP WAWANCARA I

Narasumber	Yuda Djuanda
Jabatan	Supervisor IT
Pewawancara	Meikhal Firmansyah
Tanggal	13 Maret 2009
Waktu	Jam Kerja
Tempat	Ruang Div. TI, Lantai II , Universitas Paramadina

Ins Daftar Pertanyaan

P Bagaimana mekanisme pengajuan investasi di Universitas ini, apakah ada semacam tim procurement yang akan memvalidasi form isian rencana investasi ?

N Tidak ada tim procurement. Di Universitas ini, rencana investasi dituangkan dalam RKA (Rencana Kerja Anggaran). Di dalam RKA tersebut dijabarkan rincian semua kegiatan yang akan dilakukan dalam jangka waktu 1 tahun ke depan. RKA tersebut selanjutnya diperiksa oleh Deputi Rektor Opersional & Keuangan (DROK). Setelah itu RKA tersebut dilanjutkan ke Bagian Keuangan untuk dibahas dan ditetapkan pagu anggaran untuk tahun berikutnya dan setelah itu dipresentasikan dihadapan Yayasan dan jika disetujui akan dilakukan pengesahan oleh Yayasan.

P Apakah setiap bagian atau divisi atau program studi mempunyai kesempatan untuk meng-initiate proyek atau kegiatan TI baru ?

N Sampai saat ini ya. Tiap bagian atau divisi atau program studi boleh mengajukan proyek-proyek / kegiatan yang berkaitan dengan TI. Seharusnya

aturan yang akan diterapkan adalah Deputi Rektor Operasional & Keuangan (DROK) yang mempunyai kewenangan dan yang membawahi bagian TI yang berperan untuk menentukan apakah investasi baru di bidang TI bisa dilanjutkan atau tidak.

P Seperti apa sih tata kelola TI di Universitas paramadina saat ini ?

N Tata kelola TI di Universitas paramadina ini peran pelayanan yang di titik beratkan, yaitu pelayanan untuk staf, dosen dan mahasiswa.

P Apa yang menjadi pemicu sehingga tata kelola TI di Universitas Paramadina harus baik ?

N Karena di titik beratkan pada pelayanan jadi lebih ke proses penerapan dan implementasinya.

P Tentang efisiensi, apakah ada statement dari pimpinan ?

N Iya, kita selalu berpatokan pada efisiensi. Para pimpinan itu kan harus mempertangungjawabkan ke Yayasan, berapa efisiensi yang dapat dicapai.

P Apakah ada secara tertulis atau lisan saja ?

N Penilaian efisiensi itu sebenarnya kompleks dan peniaiannya diarahkan ke sesuatu yang dinamis. Mengenai high level mereka punya pembanding untuk penggunaaan anggarannya. Misal tahun lalu anggaran TI sekian, kemudian tahun sekarang naik, namun pencapain kita seperti ini. Secara otomatis dari segi efisiensi kan menjadi naik juga.

P Inisiatif mengenai efisiensi muncul dari bawah atau dari atas ?

N Sebenarnya dari tingkat bawah juga sudah berfikir ke arah itu. Namun sebenarnya juga mengikuti pimpinan. Efisiensi tidak dihitung dari nilai uang saja tapi sumber daya manusia TI juga diperhatikan.

P Mengenai *IT Blueprint,* siapakah yang menyusun ?

N Bagian kami yaitu divisi TI dan dikonsultasikan ke Deputi Rektor Opersional & Keuangan (DROK).

P Apakah *IT Blueprint* tersebut ada detail teknisnya, misal dari sistem operasinya harus opensource ?

N Sekarang belum sampai ke tahap itu, namun inti pencapaian sudah ada di situ, termasuk SOP juga sudah mulai disusun. Karena secara intern setiap usulan proyek / kegiatan TI hanya mengikuti kebiasaan yang berdasarkan tupoksi, yakni dikumpulkan oleh tiap-tiap Direktorat yang nantinya diserahkan ke Deputi Rektor Operasional dan Keuangan (DROK) dan kemudian dibahas dan disahkan di Rektorat dan dilaksanakan oleh tiap-tiap Direktorat atau Bagian-bagian. Peranan Tim TI hanya apabila jika diperlukan, tetapi tanpa Tim TI pun Direktorat atau Bagian-bagian masih berjalan.

P Komite penyusun *IT Blueprint* tersebut berbentuk apa dan bertanggung jawab kepada siapa ?

N *IT Blue Print* yang saat ini masih dievaluasi dan disusun kembali oleh Tim TI sehingga setiap proyek / kegiatan TI diharapkan mengacu kapeda *IT Blue Print* tersebut. Namun dalam kenyataan di lapangan, ada bagian atau unit yang dapat mengusulkan proyek / kegiatan TI dengan tanpa berkoordinasi dengan Tim TI. Waktu itu namanya Komisi IT, dikoordinir oleh Program Studi TI. Mereka bertanggung jawab kepada Deputi Rektor Operasional & Keuangan (DROK).

P Untuk infrastruktur TI, muncul dari bagian atau divisi mana, termasuk pemilihan vendor ?

N Dari divisi kita, divisi TI. Untuk pemilihan barang dari divisi TI, sedangkan pengadaan barang dari bagian fasilitas. Mengenai pemilihan vendor pada waktu itu dengan sistem lelang. Kita mengundang vendor-vendor yang berkompeten untuk presentasi. Jika mereka mampu untuk memberikan

keinginan kita, kita sarankan mereka ikut lelang. Pemenang lelang akan ditentukan oleh Tim studi kelaikan proyek yang dibentuk oleh Rektorat.

P Initiate kegiatan TI / proyek itu apa harus dari kepala bagian / kepala divisi ?

N Tidak harus, bisa muncul dari usulan staff. Setiap bagian / divisi dapat membuat usulan kegiatan masing-masing setelah melakukan koordinasi *intern* baik kepada Kepala Bagian / Divisi maupun staf, selanjutnya usulan kegiatan tersebut harus disetujui oleh Kepala Bagian / Divisi setelah berkoordinasi dengan Bagian / Divisi lainnya dalam rapat *intern*. Tugas saya mengecek apakah usulan itu masih berada dalam koridor Blue print tersebut. Kemudian saya usulkan ke Deputi Rektor Operasional & Keuangan (DROK).

P Apa ada persyaratan administrasi untuk initiate proyek / kegiatan TI ?

N Cukup dengan membuat *Term of Reference* (TOR) dari suatu kegiatan TI yang berasal baik dari staf, sub bagian / sub divisi, setelah dilakukan kajian secara intern. Kemudian kumpulan *Term of Reference* (TOR) tersebut disampaikan kepada Deputi Rektor Operasional & Keuangan (DROK) untuk di kompilasi dan masuk ke pihak Rektorat. Setelah itu *Term of Reference* (TOR) dilakukan pengesahan oleh bagian Keuangan. Tahap akhir *Term of Reference* (TOR) dibawa kehadapan Yayasan untuk dilakukan pengesahan.

P Adakah parameter yang digunakan untuk mengukur hasil investasi TI di Universitas Paramadina ?

N Saya rasa hanya sekedar implementasi. Masalah pengukura kinerja TI biasanya oleh bagian lain, misal bagian akademik. Bagian ini merupakan bisnis proses nya Universitas.

P Mekanisme relasional seperti apa agar visi dan misi TI bisa sama di kepala setiap orang ?

N Usulan kegiatan untuk 1 tahun ke depan berada di bidang atau bagian masing-masing. Setelah disetujui oleh kepala bagiannya, barulah terbentuk RKA setiap bagian / program studi dan kemudian masuk ke Deputi Rektor Operasional & Keuangan (DROK) dan Rektorat untuk di bahas. Di sini dinilai dari segi efisiensi dan posting dananya.

TRANSKRIP WAWANCARA II

Narasumber	Bima Priya Santosa
Jabatan	Deputi Rektor Operaional & Keuangan (DROK)
Pewawancara	Meikhal Firmansyah
Tanggal	17 Maret 2009
Waktu	Jam Kerja
Tempat	Ruang DROK, Lantai I, Universitas Paramadina

Ins Daftar Pertanyaan

P Apakah ada keluhan sampai saat ini khususnya dari pimpinan tentang proyek-proyek / kegiatan TI di Universitas Paramadina ?

N Sampai saat ini tidak ada, mengenai perkembanga proyek-proyek yang sedang berjalan sudah dapat kita lihat perkembangan-perkembangan proyek / kegiatan TI yang sedang berjalan di project.paramadina.ac.id.

P Apakah ada keluhan kalau dari sisi produk TI seperti mengenai jaringan, internet atau yang lain mengenai produk TI ?

N Keluhan sih ga ada dari produk TI nya sendiri, yang ada keluhan itu dari teknisi. Jika listrik lagi down di server ya internet suka mati. Ya maklum di gedung server tegangan listriknya tidak stabil.

P Menurut Bapak bagian TI saat ini masih bersifat support ?

N Sampai saat ini ya masih bersifat supporting. Namun seiring dengan perkembangan SDM yang dimiliki bagian TI saat ini tidak meutup kemungkinan akan berubah tidak hanya sebagai support.