Audit Pengolahan Data Elektronik

Data Elektronik merupakan bentuk sederhana dari disrupsi teknologi yang mengharuskan pergerakan data dan informasi melalui sebuah sistem, audit atas laporan keuangan menjadi salah satu aspek yang terdampak. Transisi audit manual menjadi audit berbasis teknologi informasi dinilai lebih minim menimbulkan kesalahan dan efisiensi dari sisi biaya dan waktu.

Buku ini selain bertujuan untuk memberikan kontribusi dalam perspektif teori dan praktis juga berusaha untuk menyesuaikan dengan kebutuhan pembelajaran selama satu semester di tingkat pendidikan lanjut. Alur buku ini dimulai dari hal yang paling mendasar yaitu; pemahaman data elektronik dan faktor penunjangnya, seperti pengendalian internal yang baik dari sistem perangkat keras dan perangkat lunak. Pembahasan berikutnya masuk ke dalam kerangka audit dan beberapa contoh implementasi dari audit pengolahan data elektronik.

Audit pengolahan data elektronik memerlukan *monitoring* dan *review* secara berkala yang cukup intens, hal ini dikarenakan perkembangan teknologi informasi serta ancaman-ancaman dalam sistem informasi akan berdampak terhadap operasional dan strategis bagi perseroan.

PT RAJAGRAFINDO PERSADA
Jl. Raya Leuwinanggung No. 112
Kel. Leuwinanggung, Kec. Tapos, Kota Depok 16956
Telp 021-84311162
Email: rajapers@rajagrafindo.co.id
www.rajagrafindo.co.id

RAJAWALI PERS
DIVISI BUKU PERGURUAN TINGGI

9 786233 720243

Audit Pengolahan Data Elektronik

Aloysius Harry Mukti, M.S.Ak., Ph.D.
Dr. Istianingsih Sastrodiharjo, M.S.Ak., CA., CSRS., CSRA., CMA., CBV., CACP.

Audit Pengolahan Data Elektronik

Audit Pengolahan Data Elektronik

Audit Pengolahan Data Elektronik

Aloysius Harry Mukti, M.S.Ak., Ph.D.
Dr. Istianingsih Sastrodiharjo, M.S.Ak., CA., CSRS., CSRA., CMA., CBV., CACP.

RAJAWALI PERS
Divisi Buku Perguruan Tinggi
PT RajaGrafindo Persada
D E P O K

Perpustakaan Nasional: Katalog dalam terbitan (KDT)

Aloysius Harry Mukti dan Istianingsih Sastrodihardjo

Audit Pengolahan Data Elektronik/Aloysius Harry Mukti dan Istianingsih Sastrodihardjo—Ed. 1, Cet. 1.—Depok: Rajawali Pers, 2021.
x, 132 hlm., 23 cm.
Bibliografi: hlm. 130
ISBN 978-623-372-024-3

2021.3133 RAJ
Aloysius Harry Mukti, M.S.Ak, Ph.D.
Dr. Istianingsih Sastrodihardjo. M.S.Ak, CA., CSRS, CSRA, CMA, CBV, CACP.
AUDIT PENGOLAHAN DATA ELEKTRONIK

Cetakan ke-1, September 2021

Hak penerbitan pada PT RajaGrafindo Persada, Depok

Editor : Diah Safitri
Setter : Khoirul Umam
Desain Cover : Tim Kreatif RGP

Dicetak di Rajawali Printing

PT RAJAGRAFINDO PERSADA

Anggota IKAPI

Kantor Pusat:
Jl. Raya Leuwinanggung, No.112, Kel. Leuwinanggung, Kec. Tapos, Kota Depok 16956
Telepon : (021) 84311162
E-mail : rajapers@rajagrafindo.co.id http: //www.rajagrafindo.co.id

Perwakilan:

Jakarta-16956 Jl. Raya Leuwinanggung No. 112, Kel. Leuwinanggung, Kec. Tapos, Depok, Telp. (021) 84311162. **Bandung**-40243, Jl. H. Kurdi Timur No. 8 Komplek Kurdi, Telp. 022-5206202. **Yogyakarta**-Perum. Pondok Soragan Indah Blok A1, Jl. Soragan, Ngestiharjo, Kasihan, Bantul, Telp. 0274-625093. **Surabaya**-60118, Jl. Rungkut Harapan Blok A No. 09, Telp. 031-8700819. **Palembang**-30137, Jl. Macan Kumbang III No. 10/4459 RT 78 Kel. Demang Lebar Daun, Telp. 0711-445062. **Pekanbaru**-28294, Perum De' Diandra Land Blok C 1 No. 1, Jl. Kartama Marpoyan Damai, Telp. 0761-65807. **Medan**-20144, Jl. Eka Rasmi Gg. Eka Rossa No. 3A Blok A Komplek Johor Residence Kec. Medan Johor, Telp. 061-7871546. **Makassar**-90221, Jl. Sultan Alauddin Komp. Bumi Permata Hijau Bumi 14 Blok A14 No. 3, Telp. 0411-861618. **Banjarmasin**-70114, Jl. Bali No. 31 Rt 05, Telp. 0511-3352060. **Bali**, Jl. Imam Bonjol Gg 100/V No. 2, Denpasar Telp. (0361) 8607995. **Bandar Lampung**-35115, Perum. Bilabong Jaya Block B8 No. 3 Susunan Baru, Langkapura, Hp. 081299047094.

PRAKATA

Terlebih dahulu penulis ucapkan puji syukur kepada Tuhan Yang Maha Esa sehingga buku ini dapat selesai dan sampai di tangan pembaca yang terhormat. Buku ini disusun salah satunya untuk mengisi kekosongan referensi dalam pembelajaran Audit Pengolahan Data Elektronik, yang diharapkan dapat menjadi acuan pembelajaran selama satu semester. Buku ini dimulai terlebih dahulu dengan pemahaman pengolahan data elektronik yang dilanjutkan dengan kerangka audit dan diakhiri dengan beberapa contoh audit dalam Perusahaan.

Penghargaan dan ucapan terima kasih berikutnya penulis sampaikan kepada Ibu Istianingsih Sastrodihardjo, M.S.Ak., CA., CSRS., CSRA., CMA., CBV., CACP., atas segala bentuk dukungan dan perspektif baik akademisi maupun praktisi. Kemudian, terima kasih kami sampaikan kepada Maria Fatima, S.T., yang sudah berkontribusi aktif secara teknis dalam penyusunan buku ini.

Akhirnya, Penulis menyadari bahwa buku ini masih memerlukan peningkatan secara berkelanjutan sehingga sekiranya Penulis mengharapkan masukan yang membangun agar buku ini dapat terus bermanfaat bagi para Pembaca.

Tabanan, Bali 2021

Aloysius Harry Mukti

[Halaman ini sengaja dikosongkan]

DAFTAR ISI

1

PEMAHAMAN MENGENAI PENGOLAHAN DATA ELEKTRONIK

Pemahaman Mengenai Pengolahan Data Elektronik

1. Definisi Komputer dan Pengolahan Data

Komputer adalah serangkaian atau sekelompok mesin elektronik yang terdiri dari ribuan bahkan jutaan komponen yang dapat saling bekerja sama, serta membentuk sebuah sistem kerja yang rapi dan teliti untuk mengolah informasi menurut prosedur yang telah dirumuskan, menerima input, mengolah input, memberikan informasi, menggunakan suatu program yang tersimpan di memori komputer, dan dapat menyimpan program dan hasil pengolahan, serta bekerja secara otomatis.

Pada mulanya pengolahan informasi hampir eksklusif berhubungan dengan masalah aritmatika, tetapi komputer modern dipakai untuk banyak tugas yang tidak hanya berhubungan dengan matematika.

Data adalah kumpulan kejadian yang diangkat dari suatu kenyataan, penggambaran fakta, pengertian instruksi yang dapat disampaikan dan diolah oleh manusia atau mesin yang berupa angka-angka, huruf-huruf atau simbol-simbol khusus atau gabungan darinya. Data mentah masih belum bisa bercerita banyak, sehingga perlu diolah lebih lanjut.

Pengolahan data (*Data Processing*) adalah manipulasi pengubahan atau transformasi dari data, simbol-simbol seperti nomor dan huruf

ke dalam bentuk yang lebih berguna atau lebih berarti berupa suatu informasi untuk tujuan peningkatan kegunaannya.

Informasi adalah hasil dari kegiatan pengolahan data yang memberikan bentuk yang lebih berarti dari suatu kejadian.

Sistem Pengolahan Data adalah adalah sistem yang melakukan pengolahan data. Contoh: sistem pengolahan data penjualan, sistem pengolahan data pegawai dan lain-lain.

Pengolahan data yang diolah dengan menggunakan komputer dikenal dengan Pengolahan Data Elektronik (PDE) atau *Electronik Data Processing* (EDP).

Jadi Pengolahan Data Elektronik (PDE) atau adalah manipulasi dari data ke dalam bentuk yang lebih berarti berupa suatu informasi dengan menggunakan suatu alat elektronik, yaitu komputer.

2. Karakteristik Pengolahan Data Elektronik

a) Kompleksitas Teknis

Sistem PDE dapat ditentukan menurut kompleksitas teknisnya dan sejauh mana sistem PDE digunakan dalam organisasi. Sistem yang tidak kompleks dapat dibuat kompleks melalui salah satu atau kombinasi dari beberapa cara berikut ini.

1) Pemrosesan *on-line*: memungkinkan akses langsung ke dalam komputer. Transaksi-transaksi dimasukkan langsung ke dalam sistem sehingga *master file* dimutakhirkan pada saat entri dibuat daripada ditangguhkan seperti pada basis batch.
2) Sistem komunikasi: menghubungkan komputer secara langsung dengan para pemakai di seluruh dunia.
3) Pemrosesan yang terditribusi: funsi komputer disebar di antara beberapa CPU yang tersebar secara geografis dan dihubungkan oleh suatu sistem komunikasi.
4) Manajemen *data base*: untuk pemakaian file secara efisien dan dapat memutakhirkan file secara terus menerus, yaitu dengan cara menyortir secara fisik setiap elemen dan data hanya sekali dan pada waktu aplikasi komputer diproses datanya diformat ke dalam struktur file yang diinginkan.

5) Sistem operasi yang kompleks: memungkinkan berbagai fungsi dijalankan secara simultan.

b) Luas Pemakaian

Keluasan pemakaian PDE dalam suatu sistem juga berkaitan dengan kompleksitasnya. Biasanya bila lebih banyak fungsi perusahaan dan akuntansi dilaksanakan oleh komputer, maka sistemnya harus menjadi kompleks agar dapat menampung kebutuhan-kebutuhan pemrosesan. Cara agar sistem dapat menjadi kompleks ialah dengan menambah jumlah siklus transaksi yang dikomputerisasikan.

3. Komponen Sistem PDE

Ada empat komponen sistem PDE, yaitu:

a) Perangkat keras (*hardware*) komputer

Hardware merupakan peralatan fisik yang digunakan dalam sistem PDE. Konfigurasi *hardware* berisi lima komponen, yaitu:

1) *Central Processing Unit* (CPU).
2) Peralatan *input* (*input device*).
3) Peralatan *output*.
4) Peralatan komunikasi komputer.
5) *Secondary storage*.

b) Perangkat lunak (*software*) komputer

Perangkat lunak komputer yang terkait dengan sistem PDE adalah *system software* dan *application software*. Perangkat lunak sistem terdiri dari:

1) Sistem operasi.
2) Program *utility*.
3) *Compilers dan assemblers*.
4) Sistem manajemen basis data atau *database management system*.

c) Metode pengorganisasian data

Metode organisasi data merupakan cara bagaimana data diorganisasi dalam *file* komputer. Ada dua jenis metode pengorganisasian data yang dapat digunakan, yaitu:

1) *Traditional File Method*

   Pada metode ini, *master file* dan *file* transaksi dipisahkan untuk setiap aplikasi akuntansi atas siklus transaksi yang berbeda.

2) *Database Method*

   Database method merupakan organisasi data yang didasarkan pada kemampuan data dalam *file* untuk diakses langsung oleh berbagai program aplikasi.

d) Metode pemrosesan data

Ada tiga jenis metode pemrosesan data yang dapat digunakan, yaitu:

1) *Batch Entry/Batch Processing*

   Pada metode *batch entry/batch processing* data transaksi yang ada dikumpulkan dalam suatu batch atau kelompok. Setelah itu, data yang ada dalam kelompok tersebut dimasukkan sekaligus ke dalam komputer untuk diproses bersama-sama. Pengolahan data menggunakan *batch processing*, dilakukan dalam dua bentuk yang berbeda yang terletak pada urutan datanya. Ada dua jenis pengolahan data sesuai dengan urutan data yaitu:

   i) Data diproses secara urut seperti urutan data dalam *file*. Pada cara ini, transaksi yang terjadi perlu disortir ke dalam urutan yang sesuai dengan urutan data dalam *file*. Setelah itu pengolahan data dapat dilaksanakan.

   ii) Data diproses secara urut seperti urutan transaksi yang terjadi. Pada cara ini, transaksi yang terjadi tidak perlu disortir terlebih dahulu karena transaksi yang ada akan diproses sesuai urutan transaksi.

2) *On-Line Entry/Batch Processing*

   Pada metode o*n-line entry/batch processing*, data transaksi yang terjadi langsung dimasukkan melalui terminal, tetapi tidak langsung diproses. Data yang dimasukkan melalui terminal, disimpan terlebih dahulu dalam suatu *file* transaksi menunggu saat pemrosesan. Validitas transaksi akan diverifikasi terlebih dahulu sebelum dicatat dalam file transaksi. Pengolahan data yang menggunakan *batch processing*, dilakukan sekaligus oleh komputer.

Metode *on-line entry/batch processing* dapat dibedakan menjadi dua cara, yaitu:

i) Pengecekan validitas dilakukan dengan menggunakan data referensi yang ada dalam file.

ii) Pengecekan validitas dilakukan dengan menggunakan program-program yang berisi nilai-nilai tertentu.

3) *On-Line Entry /On-Line Processing*

Pada metode *on-line entry/on-line processing* data transaksi yang terjadi langsung dimasukkan melalui terminal untuk langsung di proses. Terminal tidak hanya merupakan alat input data, tetapi juga merupakan alat *output* data. Terminal merupakan alat *output* data karena hasil pengolahan data transaksi yang dimasukkan, dapat segera tampak pada layar komputer. Begitu data dimasukkan melalui terminal, validitas transaksi akan langsung diverifikasi. Apabila data tersebut valid maka data langsung diproses. Apabila data tersebut tidak *valid*, maka data tidak diproses, dan kesalahan yang terjadi akan disampaikan melalui tampilan layar komputer

4. Perbedaan Antara Sistem PDE dan Sistem Manual

Suatu organisasi dalam menjalankan kegiatannya perlu melakukan mekanisme pelaporan keuangan kepada pihak-pihak yang berkepentingan baik untuk internal perusahaan maupun kepada pihak-pihak di luar perusahaan. Suatu oraganisasi juga perlu memastikan efektivitas dan efisiensi kegiatan-kegiatan operasionalnya. Organisasi juga wajib mematuhi segala peraturan atau ketentuan yang mengikat aktivitas organisasi tersebut. Usaha untuk menilai keandalan laporan keuangan, efektivitas dan efisiensi kegiatan, serta kepatuhan terhadap peraturan inilah area-area yang menjadi cakupan *auditing*. Dari berbagai area *auditing* itulah akhirnya muncul istilah-istilah seperti *financial audit*, *operational audit*, dan *compliance audit*.Arens mendefinisikan *auditing* sebagai suatu proses sistematik untuk memperoleh dan mengevaluasi bukti-bukti secara objektif berdasarkan asersi-asersi kegiatan ekonomi suatu entitas dan menentukan tingkat kesesuaian antara asersi-asersi tersebut dengan kriteria yang telah ditetapkan selanjutnya mengomunikasikan hasilnya kepada pihak yang berkepentingan.

Kegiatan ekonomi sutu entitas tersebut mengalami perubahan seiring dengan kemajuan teknologi. Perubahan-perubahan juga terjadi dalam pengolahan data yang dilakukan organisasi. Menurut Gore dan Stubbe (1979) tahap awal pengolahan data dilakukan melalui sistem manual dengan menggunakan pena atau tinta, selanjutnya pengolahan data dilakukan secara mekanik dengan alat bantu semacam kalkulator dan register kas, tahap berikutnya adalah sistem pengolahan data secara elektro mekanis dengan menggunakan listrik pada berbagai macamm mesin penghitungan dan mesin pembukuan termasuk mesin-mesin pelubang kartu, tahap terakhir adalah sistem pengolahan data secara elektronik dengan bantuan komputer. Tahap terakhir inilah yang sering disebut dengan Pengolahan Data Elektronik (PDE) atau *Electronic Data Processing* (EDP). Basalamah (2008) Mengartikan PDE sebagai serangkaian kegiatan dengan menggunakan komputer untuk mengubah informasi yang masih mentah (data) menjadi informasi yang berguna yang sesuai dengan tujuannya. Rangkaian kegiatan pengolahan data tersebut terdiri dari lima bagian, yaitu: *inputting, storing, processing, outputting*, dan *controlling*.

Lingkup pengertian *auditing* PDE ditafsirkan berbeda oleh beberapa penulis. Weber menyatakan bahwa *auditing* PDE *sama dengan auditing sistem informasi* yaitu suatu proses pengumpulan dan penilaian bukti untuk menentukan apakah suatu sistem komputer melindungi aktiva, mempertahankan integritas data, serta memungkinkan bagi tercapainya tujuan organisasi secara efektif dan penggunaan sumber daya secara efisien. Pengertian auditing sistem informasi di atas lebih memokuskan pada pemeriksaan terhadap aktivitas komputer atau PDE sehingga cenderung kepada audit operasional. Sedangkan Basalamah (2008) mengartikan *auditing* PDE sebagai audit terhadap informasi yang dihasilkan dari lingkungan yang terkomputerisasi. Dari pengertian auditing PDE yang terakhir ini (yang selanjutnya dijadikan dasar pembahasan) sebenarnya ada kesamaan antara *auditing* PDE dengan audit terhadap organisasi yang tidak mengolah datanya dengan menggunakan komputer atau sering disebut dengan audit konvensional.

Definisi *auditing*, auditor, dan jenis audit tidak dibedakan antara auditing PDE dengan auditing konvensional. Demikian juga mengenai tujuan audit, opini auditor, dan standar yang digunakan adalah sama di antara kedua jenis auditing tersebut. Tetapi ada karakteristik khusus

yang membedakan antara *auditing* PDE dengan konvensional. Tahap-tahap yang dijalankan dalam audit juga mempunyai sedikit perbedaan. Secara ringkas dijelaskan dalam tabel berikut:

Tabel 1.1 Perbedaan Audit PDE dan Manual

SEGI	AUDIT KOMPUTER (AUDIT PDE)	AUDIT MANUAL (KONVENSIONAL)
Audit Nature	a. Dokumen tidak dapat dilihat. b. Proses langsung masuk komputer dan terjadi secara otomatis. c. Secara serentak memenuhi beberapa tujuan.	a. Dapat dilihat b. Dilakukan secara manual dan tidak otomatis mempengaruhi laporan. c. Tidak secara serentak
Waktu yang Dibutuhkan	Lebih cepat.	Lebih lama
Sifat Kesalahan	Bersifat berulang karena proses pengolahan transaksi dilakukan dengan bantuan komputer.	Kesalahan tidak terjadi berulang.
Audit Trail	Penggunaan computer akan mengurangi bahkan menghilangkan *audit trail*.	*Audit trail* nya terlihat secara fisik bahkan kadang diarsipkan.
Proses audit	Tidak sekuensial	Sekuensial
Pemisahan Tugas	Sering tidak ada pemisahan tugas	Ada pemisahan tugas
Ketergantungan pada hardware dan software	Tergantung	Tidak tergantung
Risiko audit	Lebih tinggi	Lebih rendah
Pengendalian intern	Selain *general contro*, audit EDP juga menekankan kepada *application control*.	Lebih menekankan kepada *general control*
Keahlian auditor	Diperlukan keahlian di bidang komputer (PDE)	Tidak diperlukan keahlian di bidang komputer (PDE)
Audit Evidence	Lebih sulit dan rumit	Lebih mudah.
Cara Audit	Cara dalam mengaudit - *Audit around the computer* - *Audit through the computer* - *Audit with the computer*	Melakukan pemeriksaan berdasarkan bukti fisik (dokumen/ bukti) yang dimiliki perusahaan dengan melakukan beberapa teknik seperti konfirmasi, wawancara, prosedur analitis, dsb.

5. Kelebihan dan Kekurangan Sistem PDE Dibandingkan dengan Sistem Manual

Metode pengelolaan data dengan sistem PDE mempunyai beberapa kelebihan dan juga mempunyai beberapa kelemahan antara lain:

a) Kelebihan sistem PDE yang berkaitan dengan *auditing*:
   1) Sistem PDE dapat memberikan konsistensi yang lebih baik dalam pemrosesan data daripada sistem manual.
   2) Sistem ODE dapat memberikan laporan akuntansi yang lebih tepat waktu dan lebih efektif untuk pengawasan dan penelaahan operasi daripada sistem manual.
   3) Sistem PDE dapat mencegah kesalahan perhitungan dan penulisan data transaksi yang sering terjadi pada sistem manual.
   4) Pada sistem PDE ada fungsi pengendalian yang dimasukkan secara *built up* ke dalam komputer. Misalkan adanya password. Hal ini tidak terdapat pada sistem manual.

b) Kelemahan Sistem PDE:
   1) Sistem PDE menghasilkan jejak transaksi yang terbatas dibandingkan sistem manual. Jejak transaksi untuk keparluan audit hanya tersedia untuk jangka waktu yang pendek.
   2) Lebih sedikit bukti dokumenter mengenai kinerja prosedur pengendalian pada sistem PDE daripada sistem manual.
   3) Informasi pada sistem PDE kurang *visible* atau sulit dilihat daripada sistem manual.
   4) Pengurangan campur tangan manusia dalam sistem PDE dapat mengakibatkan tersembunyinya kesalahan yang sebenarnya dapat diamati dalam sistem manual.
   5) Informasi dalam sistem PDE lebih rawan terhadap kerusakan fisik dibandingkan sistem manual.
   6) Berbagai fungsi dapat terkonsentrasikan dalam sistem PDE sehingga mengurangi pemisahan tugas dan wewenang. Hal ini dapat berakibat sistem PDE lebih rentan dari sisi pengendalian dibandingkan sistem manual.

7) Pengubahan sistem dalam sistem PDE lebih sulit diimplementasikan dalam dikendalikan daripada sistem manual.

8) Pada sistem PDE, lebih banyak orang yang dapat mengakses sistem daripada sistem manual.

6. Faktor-faktor yang Perlu Dipertimbangkan Dalam Pengauditan Sistem PDE

Menurut IAPI (SPAP seksi 327.8-16) faktor-faktor yang harus dipertimbangkan dalam penggunaan Teknik Audit Berbantuan Komputer (TABK) adalah:

a) Pengetahuan, keahlian, dan pengalaman komputer yang dimiliki oleh auditor.

b) Tersedianya TABK dan fasilitas komputer yang sesuai. Auditor harus mempertimbangkan tersedianya TABK, kesesuaian fasilitas komputer dan sistem akuntansi serta *file* berbasis komputer yang diperlukan. Auditor dapat merencanakan untuk menggunakan fasilitas komputer yang lain bila penggunaan TABK atas komputer entitas dianggap tidak ekonomis atau tidak praktis untuk dilakukan-sebagai contoh, karena adanya ketidaksesuaian antara program paket yang digunakan oleh auditor dengan komputer entitas. Kerja sama dari karyawan entitas dapat diperoleh untuk menyediakan fasilitas pengolahan pada waktu yang tepat, untuk membantu seperti memuat dan menjalankanTABK. Ke dalam sistem entitas, dan menyediakan *copy file* data dalam format yang dikehendaki oleh auditor.

c) Ketidakpraktisan pengujian manual.

Banyak sistem akuntansi terkomputerisasi dalam melaksanakan tugas tertentu tidak menghasilkan bukti yang dapat dilihat. Dalam keadaan ini, tidaklah praktis bagi auditor untuk melakukan pengujian secara manual. Tidak adanya bukti yang dapat dilihat dapat terjadi pada berbagai tahap proses akuntansi-seperti:

1) Dokumen masukan dapat tidak ada bila order penjualan dimasukkan ke dalam sistem secara *on-line*. Di samping itu, transaksi akuntansi, seperti perhitungan potongan harga dan

bunga, dapat dipicu dengan program komputer tanpa otorisasi yang dapat dilihat untuk setiap transaksi secara individual.

2) Sistem dapat tidak menghasilkan jejak audit *(audit trail)* yang dapat dilihat untuk transaksi yang diolah melalui komputer. Surat penyerahan barang dan faktur dari pemasok dapat ditandingkan dengan suatu program komputer. Di samping itu, prosedur pengendalian program, seperti pengecekan batas kredit pelanggan, dapat menyediakan bukti yang dapat dilihat hanya atas dasar penyimpangan. Dalam hal ini, tidak terdapat bukti yang dapat dilihat bahwa semua transaksi telah diolah.

d) Laporan keluaran dapat tidak diproduksi oleh sistem. Sebagai tambahan, suatu laporan tercetak dapat hanya berisi total ringkasan sementara rincian yang mendukung laporan tersebut tetap ditahan dalam *file* komputer.

1) Efektivitas dan efisiensi

Efektivitas dan efisiensi prosedur audit dapat ditingkatkan melalui penggunaan TABK dalam memperoleh dan mengevaluasi bukti audit-seperti:

2) Beberapa transaksi dapat diuji lebih efektif untuk tingkat biaya yang sama dengan menggunakan komputer untuk memeriksa semua atau lebih banyak transaksi dibandingkan dengan jika dilaksanakan secara manual.

3) Dalam penerapan prosedur analitik, transaksi atau saldo akun dapat *di-review* dan dicetak laporannya untuk pos-pos yang tidak biasa dengan cara yang lebih efisien dengan menggunakan komputer bila dibandingkan dengan cara manual.

4) Penggunaan TABK dapat membuat prosedur pengujian substantif tambahan lebih efisien daripada jika auditor meletakkan kepercayaan atas pengendalian dan pengujian pengendalian yang bersangkutan.

Masalah yang berhubungan dengan efisiensi yang perlu dipertimbangkan oleh auditor meliputi:

i. Waktu untuk merencanakan, merancang, melaksanakan, dan mengevaluasi TABK.

ii. Jam asisten dan *review* teknis.

iii. Perancangan dan pencetakan formulir (seperti konfirmasi).

iv. Pencatatan masukan ke dalam sistem komputer dan verifikasinya.

v. Waktu pemakaian komputer.

Dalam mengevaluasi efektivitas dan efisiensi suatu TABK, auditor dapat mempertimbangkan daur hidup aplikasi TABK. Perencanaan mula-mula, perancangan, dan pengembangan suatu TABK biasanya akan memberikan manfaat terhadap audit periode berikutnya.

Saat pelaksanaan.

File komputer tertentu, seperti *file* transaksi rinci, sering kali ditahan hanya untuk jangka waktu pendek, dan mungkin tidak disediakan dalam bentuk yang dapat dibaca oleh mesin pada saat diperlukan oleh auditor. Jadi, auditor akan memerlukan pengaturan untuk mempertahankan data yang dibutuhkannya, atau ia dapat mengubah saat pekerjaannya memerlukan data tersebut.

Jika waktu yang tersedia untuk melaksanakan audit terbatas, auditor dapat merencanakan penggunaan TABK karena program tersebut akan dapat memenuhi persyaratan waktu lebih baik dibandingkan dengan prosedur lain.

[Halaman ini sengaja dikosongkan]

2

PENGENDALIAN INTERN PADA SISTEM PDE

Pengendalian dalam sistem PDE mencakup prosedur-prosedur manual dan prosedur yang dirancang dalam program komputer. Prosedur pengendalian manual dan program komputer terdiri dari pengendalian umum dan pengendalian aplikasi.

A. Pengendalian Umum

Pengendalian umum merupakan pengendalian menyeluruh yang berdampak terhadap lingkungan PDE. Pengendalian Umum berhubungan dengan keseluruhan bagian sistem PDE. Ada empat (4) jenis pengendalian umum dalam sistem PDE, yaitu:

a) Pengendalian organisasi dan operasi

Pada sistem PDE komputerlah yang melakukan penjualan, dan melaksanakan posting. Oleh karena itu, perlu pengendalian khusus pada sistem PDE. Fungsi-fungsi pada departemen PDE meliputi:

1) Manajer departemen PDE
2) Analisis sistem
3) Pemrogram
4) Operator komputer
5) Pustakawan (librarian)

6) Kelompok pengendalian data
7) Administratur database

B. Pengendalian Perancangan Sistem dan Dokumentasi

Pengendalian ini merupakan bagian integral dari metode pemisahan otoritas dan tanggung jawab yang memadai. Pengendalian pengembangan sistem berkaitan dengan pengevaluasian sistem baru, pengendalian pengubahan program, dan prosedur dokumentasi. Hal–hal yang harus diperhatikan dalam pengembangan sistem adalah:

a) Pengembangan sistem harus melibatkan departemen lain seperti pemakai sistem PDE, departemen akuntansi, dan auditeo intern.
b) Setiap tahap pengembangan sistem harus ditelaah dan disetujui oleh departemen pemakai dan manajemen.
c) Pegujian sistem yang dikembangkan, harus melibatkan kerja sama antara departemen PDE, dan departemen pemakai.
    1) Sistem yang baru harus disetujui oleh manajer PDE, administrator database, pemakai dan manajemen, sebelum diimplementasikan pada operasi normal.
    2) Perubahan-perubahan program harus disetujui sebelum diimplementasikan untuk menentukan apakah perubahan-perubahan program tersebut telah diauntorisasi, diuji, dan didokumentasikan.

Auditor menggunakan dokumentasi untuk menghasilkan sumber informasi untuk mengenai menghasilkan sumber informasi utama mengenai aliran transaksi melalui sistem dan pengendalian akuntansi terkait. Dokumentasi meliputi:

a) Deskripsi dan diagram alur dari sistem dan program.
b) Instruksi operasi bagi operator komputer.
c) Prosedur pengendalian yang telah dijalankan dengan lebih baik oleh operator dan pemakai sistem.
d) Deskripsi dan sampel *input* data dan *output* yang diperlukan.

C. Pengendalian *Hardware* dan *Software* Sistem

Pengendalian akses untuk mencegah penggunaan peralatan PDE, file data, dan program komputer tanpa autoritas. Ada tiga katagori pengendalian yang terkait erat dengan penjagan peralatan PDE, data dan program. Ketiga katagori pengendalian tersebut, meliputi:

a) Pengendalian fisik

Pengendalian fisik berkaitan dengan perlindungan fasilitas komputer. Pengendalian ini dilakukan dalam bentuk:

1) Pemberian kunci pada pintu ruang.
2) Pemberian kunci pada terminal komputer.
3) Penyimpanan file data dan *software* pada tempat yang aman agar tidak rusak atau hilang.

b) Pengendalian akses

Pengendalian akses dilakukan untuk memastikan bahwa hanya orang yang berhak dan berwewenang saja yang dapat menggunakan peralatan komputer, dan mengakses data atau program. Pengendalian ini dapat dilakukan dalam bentuk pemberian password pada komputer. Prosedur backup dan pemulihan. Pengendalian backup dan pemulihan dapat dilakukan perusahaan untuk mencegah hilangnya data atau program. Backup merupakan salinan suatu file data atau program. Backup sebaiknya disimpan di tempat terpisah dari file asli. Dengan demikian, apabila terjadi kebakaran yang menghanguskan file asli, maka file *backup* tetap ada.

c) Pengendalian Aplikasi

Pengendalian aplikasi merupakan pengendalian khusus atas aplikasi akuntansi, seperti pemrosesan penjualan atau penerimaan kas, pemrosesan gaji dan upah karyawan dan sebagainya. Pengendalian aplikasi berkaitan erat dengan tugas-tugas khusus yang dilaksanakan oleh sistem PDE. Ada tiga jenis pengendalian aplikasi dalam sistem PDE, yaitu:

1) Pengendalian Input

Pengendalian ini merupakan pengendalian prosedural yang perlu untuk menangani data dari luar komputer atau data input. Pengendalian input meliputi pengendalian terhadap:

i. Autorisasi.
ii. Pelaksanaan konversi data masukan.
iii. Koreksi kesalahan.

2) Pengendalian Pemrosesan

Pengendalian pemrosesan dirancang untuk memberikan keyakinan memadai bahwa pemrosesan bukti kas keluar yang salah dihentikan dan tidak dilakukan koreksi, maka akun kas akan overstated. Pengendalian pemrosesan meliputi:

i. *Batch control*
ii. Pengujian urutan
iii. Pengujian batas kewajaran
iv. Laporan master file
v. Pengujian penjumlahan mendatar

3) Pengendalian *Output*

Pengendalian *output* bertujuan untuk memastikan ketepatan dan kebenaran hasil pemrosesan, dan hanya personel yang mempunyai otoritas yang menerima *output*-nya. Pengendalian keluaran dapat dilaksanakan dengan:

i. Rekonsilisasi antara total *output* yang dihasilkan program komputer, dengan total input dan pemrosesan yang dihasilkan departemen yang memberikan data input bagi PDE.
ii. Perbandingan mendetail antara data *output* dengan dokumen sumber
iii. Penelahaan visual.

Pengendalian distribusi *output* dapat dilakukan dengan mengadakan password sehingga hanya yang berwenang saja yang dapat mengetahui dan mengakses suatu *output* PDE.

D. Metodologi untuk Memenuhi Standar Pekerjaan Lapangan

Standar pekerjaan lapangan kedua mengharuskan auditor untuk menghimpun pemahaman struktur pengendalian intern klien.

Metodologi yang digunakan dalam sistem PDE secara konseptual sama dengan sistem manual.

1. Perencanaan Audit

Standar pekerjaan lapangan yang pertama dari SPAK menyatakan bahwa pekerjaan audit harus direncanakan dengan sebaik-baiknya. Perencanaan memungkinkan auditor dapat melaksanakan audit secara efisien dengan biaya yang memadai, serta memungkinkan bagi auditor untuk menghindari kesalahpahaman yang mungkin timbul dengan pihak-pihak yang diaudit.

AICPA memasukkan perencanaan ini dalam tahap penelaahan pendahuluan. Penelaahan ini bertujuan untuk memperoleh pemahaman mengenai sistem akuntansi baik berbasis elektronik maupun non elektronik melalui unsur-unsur tersebut:

a) Arus transaksi dan keluaran yang signifikan

   Tujuannya adalah auditor dapat merancang dan menerapkan prosedur-prosedur yang sesuai untuk menelaah dan menilai pengendalian akuntansi.

b) Sejauh mana penggunaan komputer dalam aplikasi akuntansi

   Agar dapat memahami sejauh mana PDE digunakan dalam aplikasi akuntansi, maka auditor harus mempertimbangkan.

   1) Jumlah dan jensi transaksi yang diproses.
   2) Nilai total rupiah setiap jenis transaksi.
   3) Sifat dan sampai sejauh mana pengolahan menggunakan PDE, termasuk yang dilaksanakan oleh program komputer.
   4) Pembagian arus transaksi antara aktivitas PDE dengan non PDE.

c) Struktur dasar dari pengendalian akuntansi, baik pengendalian bagian PDE maupun pengendalian bagian pengguna. Auditor harus memperhatikan hal-hal berikut ini.

   1) Pengendalian yang ada.
   2) Pembagian tanggung jawab terhadap pengendalian di dalam sistem antara bagian PDE dan non PDE.

3) Hubungan antara pengendalian berdasarkan PDE maupun non PDE.

4) Sifat, sejauh mana dan tersedianya informasi yang memberikan jejak audit.

Metode yang digunakan untuk memperoleh pemahaman mengenai sistem akuntansi adalah dengan kuesioner dan wawancara, observasi, penelaahan terhadap dokumentansi; mentrasir transaksi-transaksi, kuesioner pengendalian serta daftar pengujian.

Secara umum penelaahan pendahuluan terdiri menjadi tiga tahapan, yaitu pengumpulan data umum, identifikasi terhadap aplikasi keuangan, dan penyiapan rencana pemeriksaan.

Pada tahapan pengumpulan data umum auditor bermaksud mengumpulkan informasi yang bersifat umum seperti struktur organisasi satuan usaha, bagan perkiraan yang ada, *hardware* dan software yang digunakan, termasuk bagan alir (*flowchart*), prosedur-prosedur yang ada serta pengamanan fisik yang dilakukan. Berdasarkan informasi umum tersebut, seharusnya auditor dapat menentukan masalah-masalah penting yang berkaitan dengan pelaksanaan pekerjaan audit, seperti banyak waktu yang diperlukan, para personel dan kecakapan yang diperlukan untuk melaksanakan pekerjaan audit, serta kapan suatu pekerjaan audit harus dilaksanakan (penjadwalan).

Pada tahapan indentifikasi terhadap aplikasi keuangan yang dapat dintukan dengan mempertimbangkan banyak hal seperti:

a) Keinginan dari pimmpinan objek pemeriksaan, yang ditentukan dalam surat penugasan.

b) Kemungkinan terjadinya *potential error.*

c) Histori keuangan di masa lalu.

Setelah tahapan di atas dilaksanakan, maka auditor dapat menyusun rencana audit antara lain meliputi lingkup audit, uraian mengenai prosedur dan pengendalian PDE yang ada, pengaruh kekuatan dan kelemahan pengendalian aplikasi yang ada, pengujian ketaatan yang mungkin dilakukan.

Dalam perencanaan ini auditor dapat menggunakan komputer untuk melakukan:

1) Perancangan audit program.
2) Pengembangan kuesioner pengendalian internal.
3) Pelaksanaan analisis terhadap risiko satuan usaha yang tengah diaudit.
4) Pelaksanaan analisis atas data keuangan.
5) Penjadwalan pekerjaan yang akan dilakukan dan biaya-biayanya.

2. Penghimpunan Pemahaman Struktur Pengendalian Intern

Pemahaman struktur pengendalian intern tersebut harus mencakup tiga elemen, yaitu: struktur pengendalian intern, pengendalian umum, dan pengendalian aplikasi. Auditor harus menilai rancangan pengedalian PDE dan menguji apakah sudah dijalankan dalam operasi.

Prosedur untuk menghimpun pemahaman semakin ekstensif bila auditor menggunakan strategi audit dengan pendekatan *lower assessed level of control risk*. Auditor harus menghimpun pemahaman yang cukup untuk memahami:

a) Kelompok transaksi operasi entitas yang di prosese dengan sistem PDE dan yang signifikan unutk laporan keuangan.
b) Catatan akuntansi, dokumen pendukung, mesin readable information dan akun khusus dalam laporan keuangan yang mencakup pemrosesan dan laporan sistem PDE.
c) Bagaimana computer digunakan dalam memproses data.
d) Jenis salah saji potensial yang dapat terjadi

Pemahaman yang dihimpun tersebut harus didokumentasikan dalam kertas kerja.

3. Pengumpulan dan pengevaluasian bukti

Penggunaan komputer oleh auditan dalam proses bisnisnya bagi auditor menimbulkan pengaruh pada bagaimana bukti harus dikumpulkan dan dievaluasi.

a) Mengumpulkan bukti mengenai keandalan sistem PDE adalah lebih kompleks, sehingga auditor harus memahami pengendalian internal di lingkungan PDE.

b) Perkembangan teknologi pengendalian berubah dengan cepat, sehingga auditor harus menyesuaikan terhadap perkembangan tersebut dalam mengumpulkan bukti mengenai keandalan pengendalian.

Dalam evaluasi bukti Weber menyebutkan:

1) Meningkatnya kerumitan sistem PDE dan teknologi pengendalian internal maka auditor juga akan menjadi lebih sulit.
2) Untuk menilai keandalan sistem berdasarkan kekuatan dan kelemahan pengendalian sistem yang bersangkutan.
3) Kesalahan PDE yang berulang-ulang menambah beban bagi auditor untuk memastikan bahwa pengendalian dalam satuan usaha sudah memadai untuk mengamankan aktiva, integritas data, efektivitas dan efisiensi sistem serta memastikan pengendalian yang ada benar-benar ada dan berfungsi.

Untuk memperoleh informasi yang dapat digunakan oleh auditor dalam mengevaluasi pengendalian internal, yaitu:

i. Penelaahan dokumentasi.
ii. Interview dengan personel PDE dan departemen pengguna.
iii. Melakukan pengamatan terhadap praktik-praktik yang dilakukan di dalam satuan usaha yang akan di audit.

3

PENGENDALIAN INTERNAL SISTEM INFORMASI

A. Pendahuluan

Pengendalian internal yang dimaksud merupakan sistem dan prosedur yang digunakan perusahaan untuk mencapai sasaran dan tujuan yang diinginkan. Sistem Pengendalian Internal juga merupakan suatu pengendalian atau pengawasan terhadap fungsi-fungsi atau bagian-bagian terkait, analisis laporan-laporan dan kebijakan dalam perusahaan termasuk stuktur organisasi yang dilakukan secara berkelanjutan. Kegiatan pada Sistem Pengendalian Internal dilakukan pada beberapa bagian yang terkait dengan fungsi pengendalian internal yang ada. Salah satu tujuan dari beberapa perusahaan yang pada umumnya bertujuan untuk menghasilkan laba yang optimal agar dapat mempertahankan kelangsungan hidupnya, memajukan serta mengembangkan usahanya ke tingkat yang lebih tinggi. Untuk itu setiap perusahaan harus membuat keputusan bisnis yang baik. Keputusan bisnis tersebut dapat dilakukan dengan menggunakan sistem internal control untuk mengarahkan kegiatan operasional perusahaan.

Pengendalian internal berperan penting dalam perusahaan karena semakin besar dan banyaknya operasi pada perusahaan, juga karena pengendalian internal merupakan suatu metode dan prosedur yang secara langsung atau tidak langsung yang dapat meminimalkan segala

penyelewengan yang mungkin dapat merugikan perusahaan.Tujuan pengendalian internal ini dapat tercapai jika unsur-unsur pengendalian internal perusahaan itu terpenuhi dengan baik, agar pengendalian internal ini berjalan dengan efektif dan efisien. Diperlukan juga bagian tertentu bertugas untuk mengawasi dan mengevaluasi efektivitas dan efisiensi dalam pengendalian internal.Untuk menunjang keefektivan suatu pengendalian internal maka salah satu unsur yang penting adalah adanya suatu bagian dalam perusahaan yang bertugas menilai kelayakan dan keefektifan pengendalian internal yang ada dan menilai kualitas kegiatan yang telah dijalankan perusahaan.

B. Definisi Pengendalian Internal

Pengendalian intern ialah suatu proses yang dipengaruhi oleh dewan komisaris, manajemen, dan personil satuan usaha lainnya, yang dirancang untuk mendapat keyakinan memadai tentang pencapaian tujuan dalam hal keandalan pelaporan keuangan, kesesuaian dengan undang-undang dan peraturan yang berlaku, serta efektivitas dan efisiensi operasi.

1) Sistem Pengendalian Intern Menurut Ahli:
   a) Mulyadi menyebutkan bahwa "sistem pengendalian intern meliputi struktur organisasi, metode dan ukuran-ukuran yang dikoordinasikan untuk menjaga kekayaan organisasi, mengecek ketelitian dan keandalan data akuntansi, mendorong efisiensi dan mendorong dipatuhinya kebijaksanaan manajemen."
   b) Romney and Steinbart (2003) pengertian pengendalian intern adalah "*Internal Control is the plan of organizations and the method of business use to safeguard assets, provide accurate and reliable information, promote and improve operational efficiency, and encourage adherence to prescribed managerial policies*."
2) Komponen Pengendalian Intern

   Pengendalian internal yang baik harus memenuhi beberapa kriteria atau unsur-unsur. Pengendalian internal terdiri dari lima komponen yang saling terkait. Komponen pengendalian internal ini antara lain:

a) Lingkungan Pengendalian (*Control Environment*)

Lingkungan pengedalian menciptakan suasana pengendalian dalam suatu organisasi dan mempengaruhi kesadaran personal organisasi tentang pengendalian. Berbagai faktor yang membentuk lingkungan pengendalian dalam suatu entitas antara lain:

1) Nilai integritas dan etika.
2) Komitmen terhadap kompetensi.
3) Dewan komisaris dan komite audit.
4) Filosofi dan gaya operasi manajemen (Struktur organisasi).
5) Pembagian wewenang dan pembebanan tanggung jawab.
6) Kebijakan dan praktik sumber daya manusia.

b) Penaksiran risiko (*risk Asessment*)

Semua organisasi memiliki risiko, dalam kondisi apa pun yang namanya risiko pasti ada dalam suatu aktivitas, baik aktivitas yang berkaitan dengan bisnis (profit dan nonprofit) maupun nonbisnis. Suatu risiko yang telah diidentifikasi dapat dianalisis dan evaluasi sehingga dapat diperkirakan intensitas dan tindakan yang dapat meminimalkannya. Maka dalam penaksiran risiko perlu diperhatikan:

1) Perubahan lingkungan operasional.
2) Personel sistem informasi baru atau perubahan sistem informasi.
3) Pertumbuhan cepat.
4) Teknologi baru.
5) Produk atau aktivitas baru.
6) PSAK baru (Pernyataan Standar Akuntansi Keuangan).

c) Informasi dan Komunikasi (*Information and communication*)

Sistem akuntansi diciptakan untuk mengidentifikasi, merakit, menggolongkan, menganalisis, mencatat, dan melaporkan transaksi suatu entitas, serta menyelenggarakan pertanggungjawaban kekayaan dan utang entitas tersebut.

d) Aktivitas Pengendalian (*Control Activities)*

Yaitu Kebijakan dan prosedur ini memberikan keyakinan bahwa tindakan yang diperlukan telah dilaksanakan untuk mengurangi risiko dalam pencapaian tujuan. Aktivitas pengendalian memiliki berbagai macam tujuan dan diterapkan dalam berbagai tingkat dan fungsi organisasi.

e) Pemantauan (*Monitoring*)

Proses penilaian kualitas kinerja pengendalian intern sepanjang waktu. Pemantauan dilaksanakan oleh personal yang semestinya melakukan pekerjaan tersebut, baik pada tahap desain maupun pengoperasian pengendalian.

3) Peran dan tanggung Jawab

Berikut ini adalah Peranan dan Tanggung Jawab dalam Pengendalian Internal:

a) Manajemen; Manajemen bertanggung jawab untuk mengembangkan dan menyelenggarakan secara efektif pengendalian internal organisasinya.

b) Dewan direksi dan komite audit; Dewan komisaris bertanggung jawab untuk menentukan apakah manajemen memenuhi tanggung jawab mereka dalam mengembangkan dan menyelenggarakan pengendalian internal.

Fungsi komite audit yang secara langsung berdampak terhadap auditor adalah:

1) Menunjuk auditor yang melaksanakan audit tahunan terhadap laporan keuangan perusahaan.
2) Membicarakan lingkup audit dengan auditor.
3) Meminta auditor untuk melakukan komunikasi langsung mengenai masalah-masalah besar yang ditemukan oleh auditor dalam auditnya.
4) Me-*Review* laporan keuangan dan laporan audit pada saat audit selesai dilakukan.

c) Auditor *Internal*; memeriksa serta mengevaluasi kecukupan pengendalian intern suatu entitas secara periodik dan membuat rekomendasi untuk perbaikan.

d) Personel entitas lainnya; menyediakan informasi kepada/ menggunakan informasi yang ada dan mengkomunikasikan masalah-masalah yang tidak sesuai dengan pengendalian dan menggunakan informasi yang dihasilkan oleh pengendalian internal harus ditetapkan dan dikomunikasikan dengan baik.

e) Auditor Independen; menemukan kekurangan dalam pengendalian yang akan dikomunikasikan kepada manajemen, komite audit, dewan direksi bersamaan dengan rekomedasi perbaikan.

f) Pihak eksternal lainnya; Pihak yang bertanggung jawab atas pengendalian internal entitas adalah badan pengatur, seperti Bank Indonesia dan Bapepam.

g) Lingkungan Pengendalian; menetapkan suasana dari suatu organisasi yang mempengaruhi kesadaran akan pengendalian dari berbagai pihak yang merupakan pondasi dari semua komponen pengendalian intern lainnya.

4. Tujuan Pengendalian Intern

Menurut AICPA (*American Institute of Certified Public Accountants*), Pengendalian Intern itu meliputi struktur organisasi dan semua cara-cara serta alat-alat yang dikoordinasikan yang digunakan di dalam perusahaan. Definisi ini menunjukkan bahwa suatu sistem pengendalian intern yang baik itu akan berguna untuk:

a) Menjaga keamanan harta milik suatu organisasi.

b) Memeriksa ketelitian dan kebenaran data akuntansi.

c) Memajukan efisiensi dalam operasi.

d) Membantu menjaga agar tidak ada yang menyimpang dari kebijakan manajemen yang telah ditetapkan lebih dahulu.

5. Karakteristik sistem pengendalian intern

Kehandalan sistem pengendalian intern harus dilandasi dengan karakteristik, yaitu:

a) Adanya pendelegasian wewenang kepada petugas tertentu untuk menyetujui transaksi dan penetapan tugas, pengecekan kepada

petugas yang lain untuk mengetahui bahwa transaksi telah disetujui oleh petugas yang berwenang.

b) Adanya penyelenggaraan akuntansi sedemikian rupa sehingga mudah dicek.

c) Adanya pendelegasian secara fisik yang tepat, termasuk penjagaan berganda terhadap aktiva yang dimiliki.

d) Adanya perifikasi secara periodik terhadap eksistensi aktiva yang dicatat.

e) Memiliki pegawai yang cakap, mempunyai kemampuan dan latihan yang cukup, sesuai dengan tingkat pertanggungjawabannya.

f) Adanya pemisahan fungsi penyimpanan aktiva dari fungsi pencatatan, dan dari pelaksanaan transaksi yang bersangkutan.

6. Dokumen Informasi Pengendalian Intern yang Berlaku

Ada tiga cara yang biasanya digunakan oleh auditor untuk mendokumentasikan informasi mengenai pengendalian intern yang berlaku dalam perusahaan:

a) Kuesioner pengendalian intern

Kuesioner merupakan cara yang banyak dipakai oleh auditor dalam mendokumentasikan informasi pengendalian intern kliennya.

b) Uraian tertulis

Ini biasanya berisi identitas karyawan yang melaksanakan suatu fungsi dan uraian terinci cara pelaksanaan fungsinya.Penggunaan uraian tertulis hanya praktis diterpkan pada audit atas laporan keuangan perusahhan yang kecil saja.

c) Bagan alir sistem

suatu sistem yang digambarkan dengan menggunakan simbol-simbol tertentu. Simbol-simbol yang dapat digunakan oleh auditor untuk membuat deskripsi pengendalian intern kliennya.

7. Pengujian Pengendalian

Untuk menguji kepatuhan terhadap pengendalian internal, auditor melakukan dua macam pengujian: Pengujian adanya kepatuhan terhadap pengendalian internal dan Pengujian tingkat kepatuhan terhadap

pengendalian internal. Berikut ini akan dijelaskan masing-masing dari kedua pengujian di atas:

a) Pengujian adanya kepatuhan terhadap pengendalian internal untuk menentukan apakah informasi mengenai pengendalian yang dikumpulkan oleh auditor benar-benar ada, auditor melakukan dua macam pengujian:
    1) Pengujian transaksi dengan cara mengikuti pelaksanaan transaksi tertentu. Dalam membuktikan adanya kepatuhan pengendalian interrnal, auditor dapat memilih transaksi tertentu, kemudian melakukan pengamatan adanya unsur-unsur pengendalian internal dalam pelaksanaan transaksi tersebut, sejak transaksi tersebut dimulai sampai dengan selesai.
    2) Pengujian transaksi tertentu yang telah terjadi dan yang telah dicatat. Dalam hal ini auditor harus memilih transaksi tertentu kemudian mengikuti pelaksanaannya sejak awal sampai selesai, melalui dokumen-dokumen yang dibuat dalam transaksi tersebut dan pencatatannya dalam catatan akuntansi.

Pengujian tingkat kepatuhan, Dalam pengujian pengendalian terhadap pengendalian internal, auditor tidak hanya berkepentingan terhadap eksistensi unsur-unsur pengendalian internal, namun auditor juga berkepentingan terhadap tingkat kepatuhan klien terhadap pengendalian internal.

[Halaman ini sengaja dikosongkan]

4

CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY (COBIT)

A. Ruang Lingkup

Ruang lingkup tata kelola TI sangat luas dan COBIT merupakan kombinasi dari prinsip-prinsip yang telah ditanamkan dan dikenal sebagai acuan model (seperti: COSO), dan disejajarkan dengan TI *balanced scorecard*. Secara komplitnya paket produk COBIT terdiri dari keluarga produk-produk COBIT, yaitu: *executive summary*, *framework*, *control objectives*, *audit guidelines*, *implementation tool set*, serta *management guidelines*, yang sangat berguna atau dibutuhkan oleh auditor, para pengguna TI, dan para manajer. Kontrol internal mencakup *policy*, struktur organisasi, praktik dan prosedur yang menjadi tanggung jawab manajemen perusahaan. Adapun ruang lingkup dalam penulisan tata kelola TI dengan COBIT ini adalah: membantu menganalisis dan menjaga profitabilitas pada lingkungan perubahan teknologi yang bergantung pada seberapa baik pengaturan kontrol yang dilakukan serta bisa digambarkan sebagai kebijakan kendali TI secara jelas, bersih, dan praktik yang baik.

B. Tujuan dan Manfaat

Dalam kerangka tata kelola perusahaan (*corporate governance*), tata kelola TI menjadi semakin utama dan merupakan bagian tidak

terpisahkan terhadap kesuksesan penerapan tata kelola perusahaan secara menyeluruh. Tata kelola TI memastikan adanya pengukuran yang efisien dan efektif terhadap peningkatan proses bisnis perusahaan melalui struktur yang menghubungkan proses-proses TI, sumber daya TI dan informasi ke arah dan tujuan strategis perusahaan.

Lebih jauh lagi, tata kelola TI memadukan dan melembagakan *best practices* dari proses perencanaan, pengelolaan, penerapan, pelaksanaan dan pendukung, serta pengawasan kinerja TI, untuk memastikan informasi perusahaan dan teknologi yang terkait lainnya benar-benar menjadi pendukung bagi pencapaian sasaran perusahaan. Dengan keterpaduan tersebut, diharapkan perusahaan mampu mendayagunakan informasi yang dimilikinya sehingga dapat mengoptimumkan segala sumber daya dan proses bisnis mereka untuk menjadi lebih kompetitif.

Dengan adanya tata kelola TI, proses bisnis perusahaan akan menjadi jauh lebih transparan, dapat dipertanggungjawabkan, serta akuntabilitas tiap fungsi atau individu semakin jelas. Tata kelola TI bukan hanya penting bagi teknis TI saja, direksi dan bahkan komisaris, yang tanggung jawabnya terhadap investasi dan pengelolaan risiko perusahaan, adalah pihak utama yang harus memastikan bahwa perusahaannya memiliki tata kelola TI. Dengan demikian, keuntungan optimum investasi TI tercapai dan sekaligus memastikan semua potensi risiko investasi TI telah diantisipasi dan dapat terkendali dengan baik. Menurut COBIT, keputusan bisnis yang baik harus didasarkan pada pengetahuan yang berasal dari informasi yang relevan, komprehensif, dan tepat waktu. Informasi seperti itu dihasilkan oleh sistem informasi yang memenuhi tujuh kriteria: efektivitas, efisiensi, kerahasiaan, keterpaduan, ketersediaan, kesesuaian terhadap rencana atau aturan, dan keakuratan informasi yang dihasilkan. Kunci utamanya adalah untuk mengelola bisnis yang menguntungkan pada kondisi lingkungan yang berubah pesat.

Adapun tujuan dari COBIT ini sendiri adalah:

1. Diharapkan dapat membantu menemukan berbagai kebutuhan manajemen yang berkaitan dengan TI,
2. Agar dapat mengoptimalkan investasi TI,
3. Menyediakan ukuran atau kriteria ketika terjadi penyelewengan atau penyimpangan. Adapun manfaat jika tujuan tersebut tercapai adalah:

a) Dapat membantu manajemen dalam pengambilan keputusan,
b) Dapat mendukung pencapaian tujuan bisnis, dan
c) Dapat meminimalisasikan adanya tindak kecurangan/fraud yang merugikan perusahaan yang bersangkutan.

C. Definisi COBIT

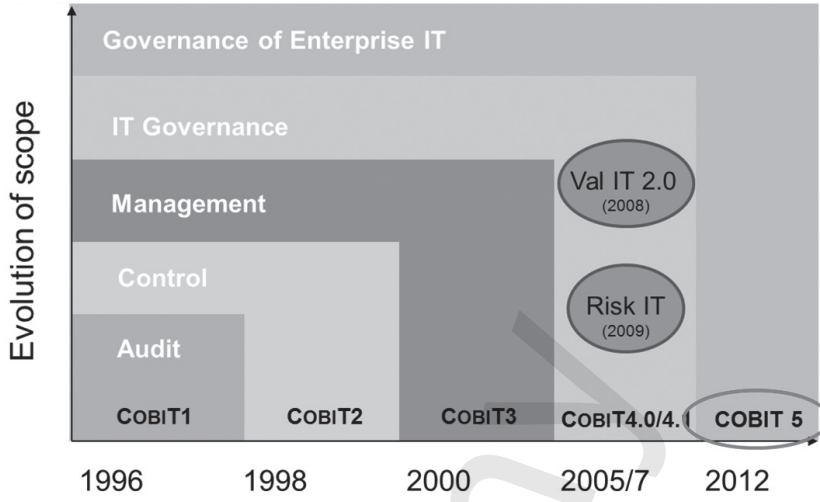
COBIT (*Control Objectives for Information and related Technology*) adalah suatu panduan standar praktek manajemen teknologi informasi dan sekumpulan dokumentasi *best practices* untuk tata kelola TI yang dapat membantu auditor, manajemen, dan pengguna untuk menjembatani pemisah (*gap*) antara risiko bisnis, kebutuhan pengendalian, dan permasalahan-permasalahan teknis.

COBIT dikembangkan oleh *IT Governance Institute* (ITGI), 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 pengguna, diharapkan dapat memanfaatkan arahan ini dengan sebaik-baiknya.

Menurut Campbell, COBIT merupakan suatu cara untuk menerapkan tata kelola TI. COBIT berupa kerangka kerja yang harus digunakan oleh suatu organisasi bersamaan dengan sumber daya lainnya untuk membentuk suatu standar yang umum berupa panduan pada lingkungan yang lebih spesifik. Secara terstruktur, COBIT terdiri dari seperangkat *control objectives* untuk bidang Teknologi Informasi, dirancang untuk memudahkan tahapan-tahapan audit bagi auditor.

D. Sejarah Perkembangan COBIT

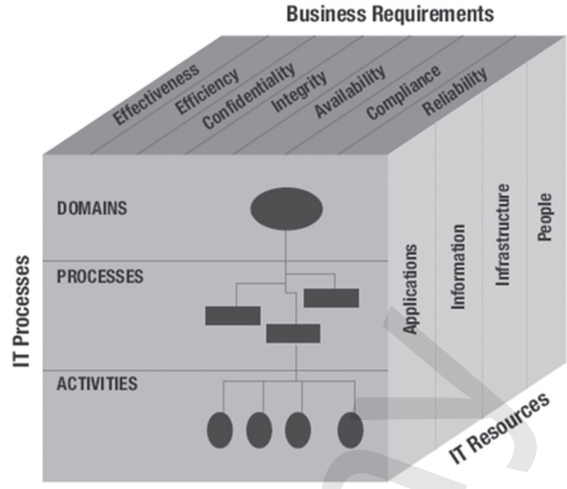
COBIT muncul pertama kali pada tahun 1996 yaitu COBIT versi 1 yang menekankan pada bidang audit, COBIT versi 2 pada tahun 1998 yang menekankan pada tahap pengendalian, COBIT versi 3 pada tahun 2000 yang berorientasi kepada manajemen, COBIT versi 4 pada bulan Desember 2005 dan versi 4.1 pada bulan Mei 2007 lebih mengarah pada tata kelola TI, dan terakhir COBIT versi 5 pada bulan Juni 2012 yang menekankan tata kelola TI pada perusahaan.



Gambar 4.1 Sejarah Perkembangan COBIT

E. Kerangka Kerja COBIT

Kerangka kerja COBIT terdiri dari tujuan pengendalian tingkat tinggi dan struktur klasifikasi secara keseluruhan, yang pada dasarnya terdiri tiga tingkat usaha tata kelola TI yang menyangkut manajemen sumber daya TI. Yaitu dari bawah, kegiatan tugas (*Activities and Tasks*) merupakan kegiatan yang dilakukan secara terpisah yang diperlukan untuk mencapai hasil yang dapat diukur. Dan selanjutnya kumpulan *Activity and Tasks* dikelompokkan ke dalam proses TI. Proses-proses TI yang memiliki permasalahan tata kelola TI yang sama akan dikelompokkan ke dalam domain. Maka konsep kerangka kerja dapat dilihat dari tiga sudut pandang, meliputi: *Information Criteria*, *IT Resources*, *IT Processes*, seperti terlihat pada gambar di bawah ini:



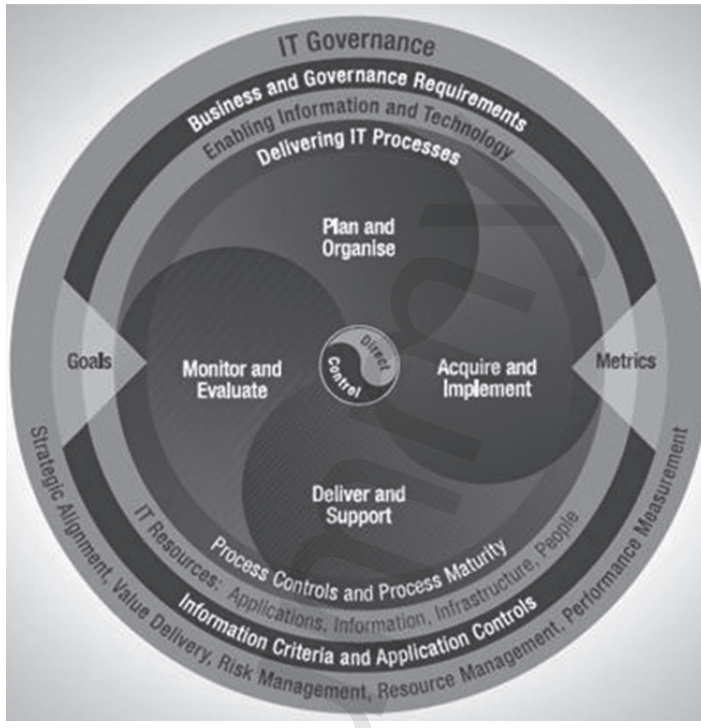
Gambar 4.2 Kubus COBIT
Sumber: (ITGI: 2007)

Lingkup kriteria informasi (*Information Criteria*) yang menjadi perhatian dalam COBIT adalah:

a) *Effectiveness*: Menitikberatkan pada sejauh mana efektivitas informasi dikelola dari data-data yang diproses oleh sistem informasi yang dibangun.
b) *Efficiency*: Menitikberatkan pada sejauh mana efisiensi investasi terhadap informasi yang diproses oleh sistem.
c) *Confidentiality*: Menitikberatkan pada pengelolaan kerahasiaan informasi secara hierarkis.
d) *Integrity*: Menitikberatkan pada integritas data/informasi dalam sistem informasi.
e) *Availability*: Menitikberatkan pada ketersediaan data/informasi dalam sistem informasi.
f) *Compliance*: Menitikberatkan pada kesesuaian data/informasi dalam sistem informasi.
g) *Reliability*: Menitikberatkan pada kemampuan/ketangguhan sistem informasi dalam pengelolaan data/informasi.

Fokus terhadap pengelolaan sumber daya teknologi informasi dalam COBIT adalah pada:

1) *Applications* (Aplikasi)
2) *Information* (Informasi)
3) *Infrastructure* (Infrastruktur)
4) *People* (Manusia/Pengguna)



Gambar 4.3 Empat Domain COBIT

Dalam memberikan informasi kepada dunia usaha sesuai dengan bisnis dan kebutuhan tata kelola teknologi informasi, model proses COBIT terdapat 4 (empat) domain yang di dalamnya terdapat 34 proses dan 318 *control objectives*, serta 1547 *control practitices*. Sehingga domain tersebut dapat diidentifikasikan yang terdiri dari 34 proses, yaitu (ITGI, 2007):

a) Domain 1: *Plan and organize (PO)* – Perencanaan dan Organisasi

Yaitu mencakup masalah mengidentifikasikan cara terbaik TI untuk memberikan kontribusi yang maksimal terhadap pencapaian tujuan bisnis organisasi. Domain ini menitikberatkan pada

proses perencanaan dan penyelarasan strategi TI dengan strategi organisasi. Domain PO terdiri dari 10 *control objectives*, meliputi:

1) PO1: *Define a strategic IT plan* (menentukan perencanaan strategi TI)
2) PO2: *Define the information architecture* (Menentukan Arsitektur Informasi)
3) PO3: *Determine technological direction* (Menentukan Arahan Teknologi)
4) PO4: *Define the IT processes, organization and relationships* (Menentukan proses-proses TI, Organisasi, dan Relasinya)
5) PO5: *Manage the IT investment* (Mengelola Investasi TI)
6) PO6: *Communicate management aims and direction* (Mengomunikasikan Tujuan dan Arah Manajemen)
7) PO7: *Manage IT human resources* (Mengelola SDM TI)
8) PO8: *Manage quality human resource* (Mengelola Mutu SDM)
9) PO9: *Asses and manage IT risks* (Menjamin dan Mengelola Risiko-risiko TI)
10) PO10: *Manage projects* (Mengelola Proyek).

b) Domain 2: *Acquire and Implement (AI)* – Akuisisi dan Implementasi

Domain ini menitikberatkan pada proses pemilihan, pengadaan dan penerapan TI yang digunakan. Pelaksanaan strategi yang telah ditetapkan, harus disertai solusi-solusi TI yang sesuai solusi TI tersebut diadakan, diimplementasikan dan diintegrasikan ke dalam proses bisnis organisasi. Di mana domain AI terdiri dari tujuh *control objectives*, meliputi:

1) AI1: *Identify automated solutions* (Mengidentifikasi otomasi solusi)
2) AI2: *Acquire and maintain application software* (Memperoleh dan memelihara aplikasi perangkat lunak)
3) AI3: *Acquire and maintain technology infrastructure* (Memperoleh dan memelihara teknologi infrastruktur)
4) AI4: *Enable operation and use* (Mengaktifkan dan menggunakan operasi)

5) AI5: *Procure IT resources* (Mendapatkan Sumber Daya TI)
6) AI6 : *Manage changes* (Mengatur Perubahan)
7) AI7 : *Install and accredit solutions and changes* (Memasang dan mengakreditasi solusi dan perubahan)

c) Domain 3: *Deliver and Support (DS)* – Penyampaian dan Dukungan

Domain ini menitikberatkan pada proses pelayanan TI dan dukungan teknisnya yang meliputi hal keamanan sistem, kesinambungan layanan, pelatihan dan pendidikan untuk pengguna, dan pengelolaan data yang sedang berjalan. Dimana domain DS terdiri dari 13 *control objectives*, meliputi :

1) DS1 : *Define and manage service levels* (Menentukan dan mengelola tingkatan layanan)
2) DS2 : *Manage third-party services* (Mengelola layanan pihak ketiga)
3) DS3 : *Manage performance and capacity* (Mengelola kinerja dan kemampuan)
4) DS4 : *Ensure continuous service* (Memastikan keberlanjutan layanan)
5) DS5 : *Ensure systems security* (memastikan keamanan sistem)
6) DS6 : *Identify and allocate costs* (Mengidentifikasi dan mengalokasikan biaya)
7) DS7 : *Educate and train users* (Memberikan Diklat kepada para pengguna)
8) DS8 : *Manage service desk and incidents* (Mengelola layanan standar dan khusus)
9) DS9 : *Manage the configuration* (Mengelola Konfigurasi)
10) DS10 : *Manage problems* (Mengelola permasalahan)
11) DS11 : *Manage data* (Mengelola Data)
12) DS12 : *Manage the physical environment* (Mengelola lingkungan fisik)
13) DS13 : *Manage operations* (Mengelola operasi-operasi)

d) Domain 4: *Monitor and Evaluate (ME)* – Pemantauan dan Evaluasi

Domain ini menitikberatkan pada proses pengawasan pengelolaan TI pada organisasi seluruh kendali-kendali yang diterapkan setiap

proses TI harus diawasi dan dinilai kelayakannya secara berkala. Domain ini fokus pada masalah kendali-kendali yang diterapkan dalam organisasi, pemeriksaan internal dan eksternal. Di mana domain ME terdiri dari 4 *control objectives*, meliputi:

1) ME1 : *Monitor and evaluate IT performance* (Memantau dan mengevaluasi kinerja TI)
2) ME2 : *Monitor and evaluate internal control* (Memantau dan mengevaluasi kendali internal)
3) ME3 : *Ensure regulatory compliance* (Memastikan kepatuhan/ kesesuaian terhadap aturan)
4) ME4 : *Provide IT Governance* (Menyediakan tata kelola TI)

Maka dengan melakukan kontrol terhadap 34 *control objectives* tersebut, organisasi dapat memperoleh keyakinan akan kelayakan tata kelola dan kendali yang diperlukan untuk lingkungan TI. Karena COBIT dirancang beriorientasi bisnis agar bisa digunakan banyak pihak, tetapi lebih penting lagi adalah sebagai panduan yang komprehensif bagi manajemen dan pemilik bisnis proses. Kebutuhan bisnis akan tercermin dari adanya kebutuhan informasi. Dan informasi itu sendiri perlu memenuhi kriteria pengendalian tertentu, untuk mencapai tujuan bisnis.

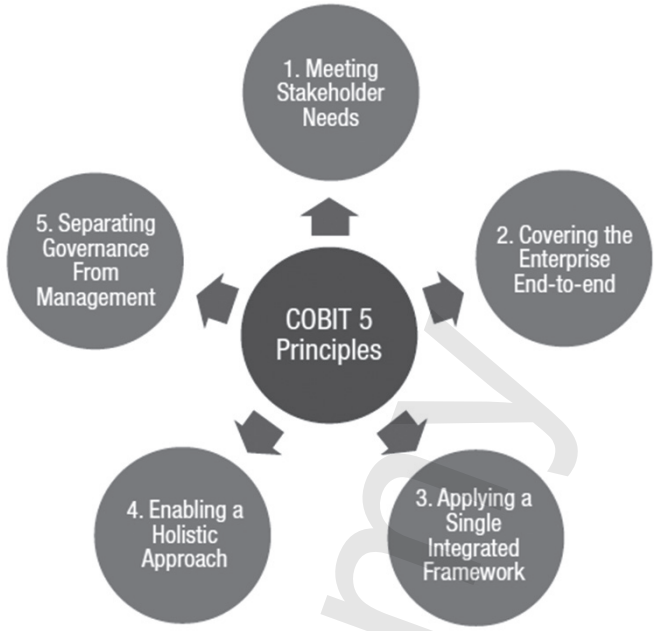
[Halaman ini sengaja dikosongkan]

5

TATA KELOLA DAN MANAJEMEN TI PERUSAHAAN

Pendahuluan

COBIT 5 merupakan sebuah kerangka menyeluruh yang dapat membantu perusahaan dalam mencapai tujuannya untuk tata kelola dan manajemen TI perusahaan. Secara sederhana, COBIT 5 membantu perusahaan menciptakan nilai optimal dari TI dengan cara menjaga keseimbangan antara mendapatkan keuntungan dan mengoptimalkan tingkat risiko dan penggunaan sumber daya. COBIT 5 memungkinkan TI untuk dikelola dan diatur dalam cara yang lebih menyeluruh untuk seluruh lingkup perusahaan, meliputi seluruh lingkup bisnis dan lingkup area fungsional TI, dengan mempertimbangkan kepentingan para *stakeholder* internal dan eksternal yang berhubungan dengan TI. COBIT 5 bersifat umum dan berguna untuk segala jenis ukuran perusahaan, baik itu sektor komersial, sektor non profit atau pada sektor pemerintahan/publik. COBIT 5 didasarkan pada lima prinsip kunci untuk tata kelola dan manajemen TI perusahaan. Kelima prinsip ini memungkinkan perusahaan untuk membangun sebuah kerangka tata kelola dan manajemen yang efektif, yang dapat mengoptimalkan investasi dan penggunaan TI untuk mendapatkan keuntungan bagi para *stakeholder*.



Gambar 5.1 Lima Prinsip dalam COBIT 5

1. Prinsip 1: Memenuhi Kebutuhan *Stakeholder*

Perusahaan ada untuk menciptakan nilai bagi para *stakeholder*-nya dengan menjaga keseimbangan antara realisasi keuntungan dan optimasi risiko dan penggunaan sumber daya. COBIT 5 menyediakan semua proses yang dibutuhkan dan pemicu-pemicu lainnya untuk mendukung penciptaan nilai bisnis melalui penggunaan TI. Oleh karena setiap perusahaan memiliki tujuan yang berbeda, sebuah perusahaan dapat mengkustomisasi COBIT 5 agar sesuai dengan konteks perusahaan itu sendiri melalui pengaliran tujuan (*goal cascade*), menerjemahkan tujuan utama perusahaan menjadi tujuan yang dapat diatur, spesifik dan berhubungan dengan TI, serta memetakan tujuan-tujuan tersebut menjadi proses-proses dan praktik-praktik yang spesifik. Perusahaan memiliki beberapa *stakeholder*, dan 'penciptaan nilai' memiliki arti yang berbeda-beda bagi masing-masing *stakeholder*, bahkan kadang bertentangan. Tata kelola berhubungan dengan negoisasi dan memutuskan di antara beberapa kepentingan dari para *stakeholder* yang berbeda-beda. Oleh karena itu, sistem tata kelola harus mempertimbangkan seluruh *stakeholder* ketika membuat keputusan mengenai keuntungan, risiko, dan penugasan sumber daya. Untuk setiap

keputusan, pertanyaan berikut ini dapat dan harus dipertanyakan: Untuk siap keuntungan tersebut? Siapa yang menanggung risiko? Sumber daya apa saja yang dibutuhkan? Setiap perusahaan beroperasi dalam konteks yang berbeda-beda. Konteks tersebut ditentukan oleh faktor eksternal (pasar, industri, geopolitik, dan sebagainya) dan faktor internal (budaya, organisasi, selera risiko, dan sebagainya), dan memerlukan sebuah sistem tata kelola dan manajemen yang disesuaikan. Kebutuhan *stakeholder* harus dapat ditransformasikan ke dalam suatu strategi tindakan perusahaan. Alur tujuan dalam COBIT 5 adalah suatu mekanisme untuk menerjemahkan kebutuhan *stakeholder* menjadi tujuan-tujuan spesifik pada setiap tingkatan dan setiap area perusahaan dalam mendukung tujuan utama perusahaan dan memenuhi kebutuhan *stakeholder*, dan hal ini secara efektif mendukung keselarasan antara kebutuhan perusahaa dengan solusi dan layanan TI.

Alur tujuan COBIT 5 digambarkan sebagai berikut:

Gambar 5.2 Alur Tujuan dalam COBIT 5

a) Langkah 1. Penggerak *stakeholder* mempengaruhi kebutuhan *stakeholder*

   Kebutuhan *stakeholder* dipengaruhi oleh sejumlah penggerak, di antaranya perubahan strategi, lingkungan bisnis dan peraturan yang berubah, dan munculnya teknologi baru.

b) Langkah 2. Kebutuhan *stakeholder* diturunkan menjadi tujuan perusahaan

   Kebutuhan *stakeholder* dapat berhubungan dengan sejumlah tujuan-tujuan umum perusahaan. Tujuan-tujuan perusahaan tersebut telah dikembangkan menggunakan dimensi *Balanced Scorecard* (BSD), dan BSD tersebut merepresentasikan sebuah daftar tujuan-tujuan yang umum digunakan di mana sebuah perusahaan dapat mendefinisikan untuk dirinya sendiri. Meskipun daftar tersebut tidak lengkap menyeluruh, kebanyakan tujuan-tujuan perusahaan tertentu dapat dipetakan secara mudah menjadi satu atau lebih tujuan umum perusahaan.

c) Langkah 3. Tujuan perusahaan diturunkan menjadi tujuan yang berhubungan dengan TI

   Pencapaian tujuan perusahaan memerlukan sejumlah hasil-hasil yang berhubungan dengan TI, yang diwakili oleh tujuan-tujuan TI. Tujuan-tujuan yang berhubungan dengan TI disusun dengan dimensi-dimensi dalam IT BSC. COBIT 5 mendefinisikan 17 tujuan yang berhubungan dengan TI.

d) Langkah 4. Tujuan TI diturunkan menjadi tujuan pemicu (*enabler goal*)

   Mencapai tujuan TI membutuhkan penerapan yang sukses dan penggunaan sejumlah pemicu. Pemicu meliputi proses, struktur organisasi dan informasi, dan untuk tiap pemicu, serangkaian tujuan yang spesifik dapat didefinisikan untuk mendukung tujuan TI.

IT BSC Dimension	Information and Related Technology Goal	
Financial	01	Alignment of IT and business strategy
	02	IT compliance and support for business compliance with external laws and regulations
	03	Commitment of executive management for making IT-related decisions
	04	Managed IT-related business risk
	05	Realised benefits from IT-enabled investments and services portfolio
	06	Transparency of IT costs, benefits and risk
Customer	07	Delivery of IT services in line with business requirements
	08	Adequate use of applications, information and technology solutions
Internal	09	IT agility
	10	Security of information, processing infrastructure and applications
	11	Optimisation of IT assets, resources and capabilities
	12	Enablement and support of business processes by integrating applications and technology into business processes
	13	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards
	14	Availability of reliable and useful information for decision making
	15	IT compliance with internal policies
Learning and Growth	16	Competent and motivated business and IT personnel
	17	Knowledge, expertise and initiatives for business innovation

Gambar 5.3 Tujuan Perusahaan dan Tujuan *IT-related* dalam COBIT 5

2. Prinsip 2: Melingkupi Seluruh Perusahaan

COBIT 5 mencakup semua fungsi dan proses dalam perusahaan. COBIT 5 tidak hanya fokus pada 'fungsi TI', namun memperlakukan informasi dan teknologi yang berhubungan dengannya sebagai suatu aset yang perlu ditangani oleh semua orang dalam perusahaan seperti juga aset-aset perusahaan yang lain. COBIT 5 mempertimbangkan semua pemicu untuk tata kelola dan manajemen yang berhubungan dengan TI agar dapat digunakan secara menyeluruh dalam perusahaan, termasuk semua orang dan semua hal –internal dan eksternal– yang berhubungan dengan tata kelola dan manajemen informasi dan TI perusahaan.

COBIT 5 mengintegrasikan tata kelola TI perusahaan ke dalam tata kelola perusahaan. Oleh karena itu, sistem tata kelola untuk TI perusahaan yang diusulkan dalam COBIT 5 ini dapat terintegrasi secara baik ke dalam sistem tata kelola manapun. COBIT 5 meliputi semua fungsi dan proses yang dibutuhkan untuk mengatur dan mengelola informasi perusahaan dan teknologi di mana informasi tersebut diproses. COBIT 5 meyediakan suatu pandangan yang menyeluruh dan sistemik pada tata kelola dan manajemen TI perusahaan, berdasarkan sejumlah pemicu/*enabler*. Pemicu-pemicu tersebut melingkupi seluruh perusahaan dari ujung ke ujung, termasuk semua hal dan semua orang, internal dan eksternal, yang berhubungan dengan tata kelola dan manajemen informasi dan TI perusahaan, termasuk juga aktivitas-aktivitas dan tanggung jawab dari kedua fungsi, yaitu fungsi TI dan fungsi bisnis selain TI. Pendekatan yang digunakan dalam tata kelola adalah sebagai berikut:

a) Pemicu Tata Kelola

   Pemicu Tata Kelola adalah sumber daya organisasi untuk tata kelola, seperti kerangka kerja, prinsip, struktur, proses, dan praktik. Sumber daya perusahaan juga termasuk sebagai pemicu tata kelola, seperti misalnya kemampuan layanan (infrastruktur TI, aplikasi, dan sebagainya), manusia dan informasi. Kekurangan sumber daya atau pemicu dapat mempengaruhi kemampuan suatu perusahaan dalam menciptakan sebuah nilai.

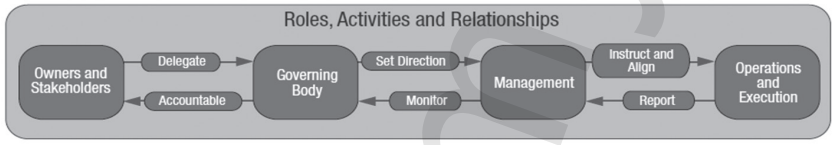
b) Ruang Lingkup Tata Kelola

   Tata kelola dapat diterapkan pada seluruh perusahaan, suatu entitas, suatu aset yang *tangible* maupun *intangible*, dan sebagainya. Maka dimungkinkan untuk dapat menentukan pandangan yang berbeda

terhadap tata kelola seperti apa sajakah yang dapat diterapkan dalam perusahaan, dan hal tersebut sangat penting untuk menentukan ruang lingkup sistem tata kelola dengan tepat dan baik.

c) Peran, Aktivitas, dan Hubungan

Elemen terakhir adalah peranan, aktivitas, dan hubungan tata kelola. Hal ini menentukan siapa yang terlibat dalam tata kelola, bagaimana mereka terlibat, apa yang mereka lakukan dan bagaimana mereka berinteraksi dalam suatu ruang lingkup sistem tata kelola. Dalam COBIT 5, perbedaan jelas dibuat antara aktivitas tata kelola dan aktivitas manajemen, dan juga mengenai interaksi antar keduanya dan para pelaku yang terlibat di dalamnya.



Gambar 5.4 Peranan, Aktivitas, dan Hubungan Tata Kelola dan Manajemen

3. Prinsip 3: Menerapkan Suatu Kerangka Tunggal yang Terintegrasi

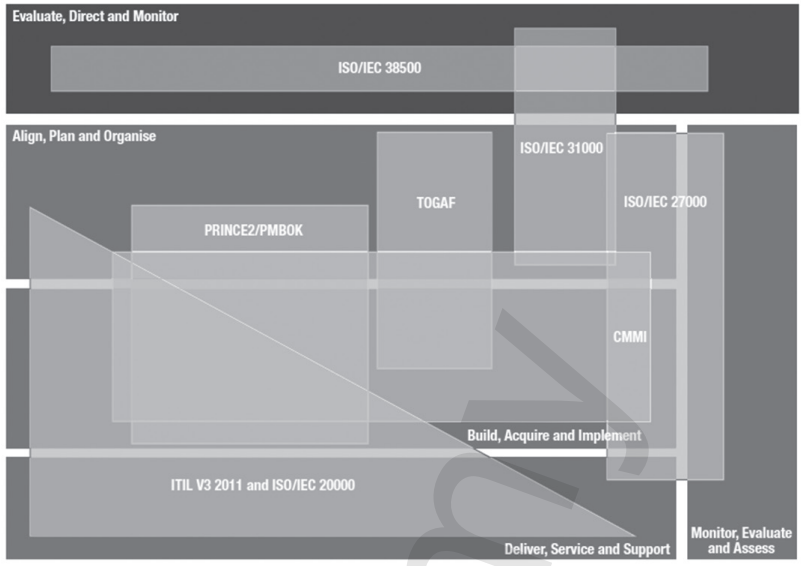
Ada beberapa standar dan *best practices* yang berhubungan dengan TI, masing-masing menyediakan panduan dalam sebuah bagian dari aktivitas TI. COBIT 5 adalah sebuah kerangka tunggal dan terintegrasi karena:

a) COBIT 5 selaras dengan standar dan kerangka kerja lain yang relevan dan terbaru, dan hal tersebut memungkinkan perusahaan untuk menggunakan COBIT 5 sebagai kerangka kerja untuk tata kelola dan manajemen secara menyeluruh dan terintegrasi,

b) COBIT 5 sangat lengkap menjangkau semua lingkup perusahaan, menyediakan dasar untuk secara efektif mengintegrasikan kerangka kerja, standar, dan praktik lain yang telah digunakan,

c) COBIT 5 menyediakan sebuah arsitektur sederhana untuk menyusun bahan panduan dan menghasilkan produk yang konsisten,

d) COBIT 5 mengintegrasikan semua pengetahuan sebelumnya yang terpecah-pecah dalam kerangka ISACA yang berbeda-beda. ISACA sebelumnya telah mengembangkan beberapa kerangka kerja seperti COBIT, Val IT, Risk IT, BMIS, ITAF, dan lain-lain. COBIT 5 mengintegrasikan semua pengetahuan tersebut.



Gambar 5.5 Integrasi Standar dan Kerangka Kerja Lain dalam COBIT 5

4. Prinsip 4: Menggunakan Sebuah Pendekatan yang Menyeluruh

Tata kelola dan manajemen TI perusahaan yang efektif dan efisien memerlukan suatu pendekatan yang menyeluruh, dan melibatkan beberapa komponen yang saling berinteraksi. COBIT 5 mendefinisikan serangkaian pemicu untuk mendukung implementasi sistem yang komprehensif tentang tata kelola dan manajemen TI perusahaan. Pemicu secara luas didefinisikan sebagai sesuatu hal apa pun yang dapat membantu mencapai tujuan perusahaan. Pemicu adalah faktor yang –secara individual maupun kolektif– mempengaruhi apakah sesuatu dapat berjalan dengan baik, dalam kasus ini adalah apakah tata kelola dan manajemen TI perusahaan dapat berjalan dengan baik.

COBIT 5 menjelaskan tujuh kategori pemicu:

a) Prinsip, Kebijakan, dan Kerangka Kerja, merupakan sarana untuk menerjemahkan kebiasaan-kebiasaan yang diinginkan menjadi suatu panduan praktik untuk manajemen sehari-hari.

b) Proses, menjelaskan serangkaian aktivitas dan praktik yang teratur untuk mencapai tujuan tertentu dan menghasilkan *output* dalam mendukung pencapaian tujuan TI secara menyeluruh.

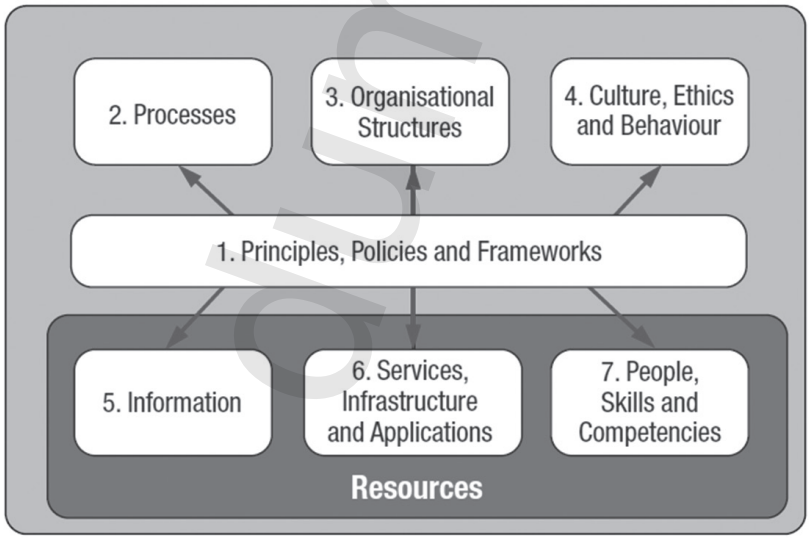
c) Struktur Organisasi, merupakan kunci untuk pengambilan keputusan dalam suatu perusahaan.

d) Budaya, Etika, dan Kebiasaan, sering diremehkan sebagai salah satu kunci sukses dalam aktivitas tata kelola dan manajemen.

e) Informasi, menyebar ke seluruh organisasi dan termasuk semua informasi yang dihasilkan dan digunakan oleh perusahaan. Informasi dibutuhkan untuk menjaga agar perusahaan dapat berjalan dan dikelola dengan baik.

f) Layanan, Infrastruktur, dan Aplikasi, termasuk infrastruktur, teknologi, dan aplikasi yang menyediakan layanan dan pengolahan teknologi informasi bagi perusahaan.

g) Manusia, Kemampuan, dan Kompetensi, berhubungan dengan manuasia dan diperlukan untuk keberhasilan semua aktivitas dan untuk menentukan keputusan yang tepat serta untuk mengambil tindakan korektif.



Gambar 5.6 Tujuh Kategori Pemicu dalam COBIT 5

Setiap perusahaan harus selalu mempertimbangkan bahwa pemicu-pemicu tersebut saling berhubungan satu dengan yang lainnya.

Masing-masing pemicu memerlukan input dari pemicu yang lain untuk dapat berfungsi secara efektif, misalnya proses memerlukan informasi, struktur organisasi memerlukan kemampuan dan kebiasaan. Masing-masing pemicu juga memberikan *output* yang bermanfaat bagi pemicu yang lain, misalnya proses menghasilkan informasi, kemampuan dan kebiasaan untuk membuat proses tersebut efisien.

5. Prinsip 5: Pemisahan Tata kelola dari Manajemen

Kerangka COBIT 5 memuat suatu perbedaan yang jelas antara tata kelola dan manajemen. Dua disiplin yang berbeda ini juga meliputi aktivitas yang berbeda, memerlukan struktur organisasi yang berbeda dan melayani tujuan yang berbeda pula. Kunci perbedaan antara tata kelola dan manajemen menurut COBIT 5 adalah:

a) Tata kelola menjamin bahwa kebutuhan *stakeholder*, kondisi-kondisi, dan pilihan-pilihan selalu dievaluasi untuk menentukan tujuan perusahaan yang seimbang dan disepakati untuk dicapai; menentukan arah melalui penentuan prioritas dan pengambilan keputusan; dan memantau pemenuhan unjuk kerja terhadap tujuan dan arah yang disepakati. Pada kebanyakan perusahaan, tata kelola secara menyeluruh adalah tanggung jawab para direksi di bawah pimpinan seorang *chairperson*. Tanggung jawab tata kelola yang lebih spesifik dapat didelegasikan kepada sebuah struktur organisasi khusus pada sebuah tingkatan yang lebih memerlukannya, biasanya pada perusahaan yang besar dan kompleks.
b) Manajemen bertugas untuk merencanakan, membangun, menjalankan, dan memantau aktivitas dalam rangka penyelarasan dengan arah perusahaan yang telah ditentukan oleh badan pengelola (tata kelola), untuk mencapai tujuan perusahaan. Pada kebanyakan perusahaan, manajemen adalah tanggung jawab manajemen eksekutif di bawah pimpinan seorang CEO.

Berdasarkan definisi tata kelola dan manajemen, jelas terlihat bahwa keduanya meliputi aktivitas-aktivitas yang berbeda dengan tanggung jawab yang berbeda. Bagaimanapun juga, berdasarkan peranan tata kelola – untuk mengevaluasi, mengarahkan, dan memantau – diperlukan suatu interaksi antara tata kelola dan manajemen untuk menghasilkan sistem tata kelola yang efektif dan efisien.

6

AUDIT ELECTRONIC DATA PROCESSING

A. Pengertian *Auditing*

Auditing adalah proses pengumpulan dan pengevaluasian bahan bukti tentang informasi yang dapat diukur mengenai suatu entitas ekonomi yang dilakukan seorang yang kompeten dan independen untuk dapat menentukan dan melaporkan kesesuaian informasi dimaksud dengan kriteria-kriteria yang telah ditetapkan[1].

B. Pengertian Audit Sistem Informasi

Ron Weber (1999,10) mengemukakan bahwa Audit Sistem Informasi adalah :

> *"Information systems auditing is the process of collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, allows organizational goals to be achieved effectively, and uses resources efficiently"* [2].

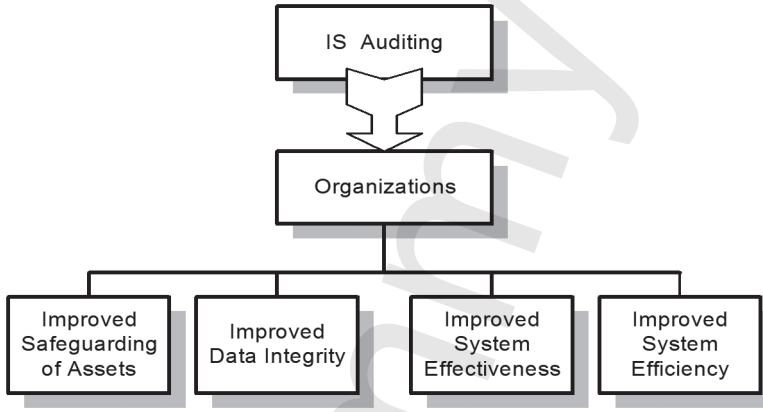
(Audit Sistem Informasi adalah proses pengumpulan dan penilaian bukti-bukti untuk menentukan apakah 'sistem komputer' dapat mengamankan aset, memelihara integritas data, dapat mendorong pencapaian tujuan organisasi secara efektif dan menggunakan sumber daya secara efisien).

C. Dampak Fungsi Audit Sistem Informasi Pada Suatu Organisasi

1. Objek Perlindungan Aset (*Asset Safeguarding Objectives*)

a) Aset SI di dalam organisasi adalah H/W, S/W, Fasilitas, User (*Knowledge*), file data, dokumentasi sistem, dan persediaan barang.

b) Sebaiknya semua aset harus dilindungi oleh sistem pengendalian internal.



Gambar 6.1 Dampak Fungsi Audit Sistem Informasi Pada Suatu Organisasi

2. Objek Integritas Data (*Data Integrity Objectives*)

a) Integritas data adalah merupakan konsep dasar di dalam audit SI. Data terdiri dari atribut-atribut yang harus berisi: lengkap (*completeness*), dapat dipercaya (*soundness*), bersih (*purity*), and benar (*veracity*).

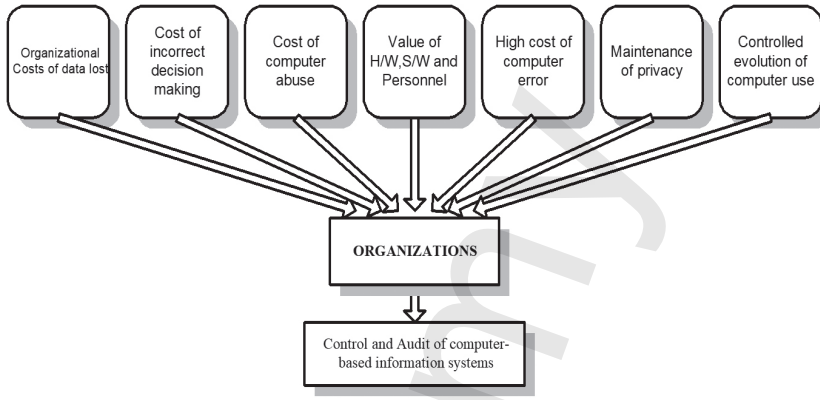
b) Jika integritas data tidak dipelihara, maka organisasi tidak akan mendapatkan representasi data yang benar untuk suatu aktivitas, akibatnya organisasi tidak dapat berkompetisi.

3. Objek Efektivitas Sistem (*System Effectiveness Objectives*)

a) Audit efektivitas sering dilakukan setelah sistem berjalan untuk beberapa waktu. Manajemen membutuhkan hasil audit efektivitas untuk mengambil keputusan apakah sistem terus dijalankan atau dihentikan sementara untuk proses modifikasi.

4. Objek Efisiensi Sistem (*System Efficiency Objectives*)

a) Efisiensi SI dilakukan dengan cara menggunakan sumber daya yang minimum untuk menyelesaikan suatu tujuan objek (pekerjaan). Variasi sumber daya terdiri dari mesin, waktu, peripheral, S/W sistem, dan pekerja.



Gambar 6.2 Faktor-faktor yang Mempengaruhi Organisasi Sehingga Perlu Melakukan Audit dan Pengendalian Terhadap SI

D. Kenapa Organisasi Perlu Melakukan Audit dan Pengendalian Terhadap SI

1. *Organizational Costs of Data Loss*

a) Data dapat menyebabkan kebutuhan sumber daya menjadi kritis untuk keberlangsungan operasional organisasi (baik untuk memberikan gambaran masa lalu,masa kini dan masa yang akan datang).

b) Jika data akurat, maka organisasi akan mempunyai kemampuan untuk beradaptasi dan bertahan dalam lingkungan yang berubah. Jika tidak (data hilang), maka organisasi akan mengalami kehilangan data yang cukup penting.

c) Contoh jika data master barang di suatu toko swalayan rusak, maka kasir tidak dapat melakukan transaksi pembelian yang dilakukan oleh konsumen.

2. *Cost of Incorrect Decision Making*

a) Untuk membuat keputusan yang berkualitas dan dapat dipercaya, maka perlu didukung oleh data yang akurat melalui sistem informasi berbasis komputer.

b) Termasuk: deteksi, investigasi, dan koreksi proses yang diluar kontrol (*connection of out-of-control process*)

c) Akibat data yang salah akan mempunyai dampak terhadap minat investor terhadap perusahaan. Contoh: jika penyediaan laporan keuangan salah (*inaccurate financial information*), maka investor akan membatalkan atas keputusan investasinya.

d) Penting juga diperhatikan tentang 'aturan-aturan keputusan yang akurat (*accurate decision rules*). Contoh jika aturan pengambilan keputusan (*decision rule*) dalam sistem pakar untuk mendukung diagnosis, salah, mengakibatkan dokter akan salah dalam memberikan keputusan/pemberian resep kepada pasiennya, ini akan berakibat fatal.

3. *Cost of Computer Abuse*

a) Sebagian besar sebab yang mendorong pengembangan fungsi audit SI di perusahaan adalah akibat seringnya terjadi penyalahgunaan komputer.

b) Penyalahgunaan komputer: "segala kejadian yang berhubungan dengan teknologi komputer yang mengakibatkan kerugian pada korban atau mengakibatkan kehilangan yang diakibatkan oleh pelaku kejahatan untuk mencari keuntungan"

c) Sebagian besar tipe penyalahgunaan komputer adalah:

   1) *Hacking*: seseorang yang tidak mempunyai akses otoritas terhadap sistem komputer untuk membaca, memodifikasi atau menghapus program atau data untuk mengacaukan proses.

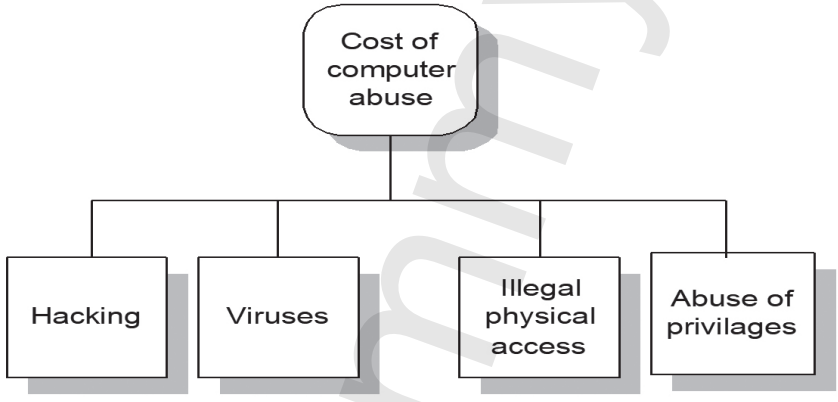
   2) Virus: adalah program yang menyerang file *executable*, area sistem atau disk, atau file data yang berisi macro yang mengakibatkan kekacauan operasi komputer atau kerusakan data/program.

   3) *Illegal Physical Access*: seseorang yang mengambil keuntungan melalui akses fisik secara ilegal terhadap fasilitas komputer.

Contoh memasuki ruang komputer atau ruang terminal secara ilegal, merusak H/W, atau copy program dan data yang bukan merupakan wewenangnya.

4) *Abuse of Privilages*: seseorang yang menggunakan hak-hak istimewanya untuk maksud dan tujuan yang bukan merupakan otoritasnya. Contoh: membuat copy data yang rahasia (sensitif) akan tetapi tidak meminta ijin atau persetujuan kepada yang berwenangnya.

Menurut survei Benbow (1990): 80% penyalahgunaan komputer diakibatkan oleh 'pegawai intern'.



Gambar 6.3 *Cost of Computer Abuse*

4. Konsekuensi Penyalahgunaan Komputer

d) *Destruction of asset* (perusakan aset): Hardware, software, data, fasilitas, dokumentasi atau persediaan barang dapat dirusak.

e) *Theft of asset* (pencurian asset): Hardware, software, data, dokumentasi, atau persediaan barang dapat dipindahkan secara ilegal.

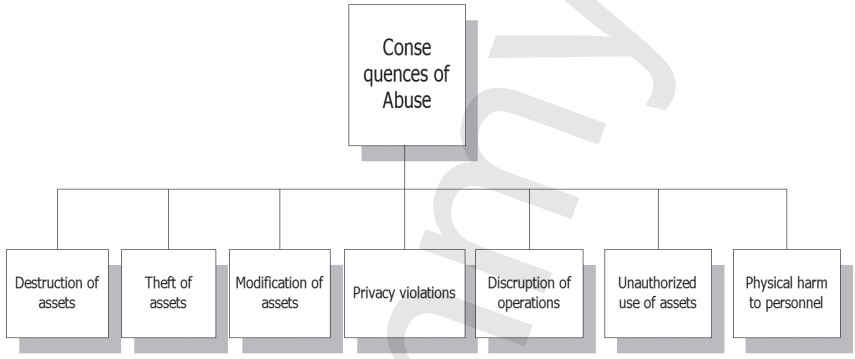
f) *Modification of asset*: Hardware, software, data atau dokumentasi dimodifikasi dengan cara yang tidah syah

g) *Privacy violaction* (pelanggaran privasi): privasi mengenai data seseorang atau organisasi di gunakan untuk kepentingan yang tidak sah.

h) *Disruption of Operations* (pengacauan operasi): operasi fungsi sehari-hari (‘*day-to-day*’) SI dapat terhenti sementara yang diakibatkan oleh operasi yang dikacaukan.

i) *Unauthorized use of asset* (penyalahgunaan otorisasi aset): Hardware, software, data, fasilitas, dokumentasi atau persediaan barang digunakan untuk maksud yang tidak sah. contoh penggunaan komputer dinas di kantor untuk maksud private atau konsultasi.

j) *Physical harm to personnel* (kejahatan fisik terhadap personal): personal/pegawai dapat menderita akibat kejahatan fisik.



Gambar 6.4 *Consequences of Abuse*

5. *Value of computer H/W,S/W, Personnel*

a) Data, H/W, S/W dan personal adalah merupakan sumber daya kritis organisasi.

b) Beberapa organisasi telah menginvestasikan ratusan miliar dollar untuk itu.

6. *High Cost of Computer Error*

a) Komputer saat ini mempunyai peranan/fungsi penting dengan lingkungan sosial. Contoh monitor digunakan untuk memantau pasien, memonitor missile, pengendali reaktor nuklir, dan lain-lain. Akibatnya jika komputer ‘error’, maka akan mengakibatkan kerugian yang sangat besar (mahal).

b) Contoh: 257 orang meninggal di pegunungan antartika, akibat error pada sistem yang diakibatkan oleh pekerjaan ‘iseng’ seseorang

yang mengganti isi/data sistem komputer yang terkait dengan penerbangan.

7. *Maintenance of Privacy*

Sebagian besar data dikumpulkan, merupakan data individu seperti: data pembayar pajak, *credit, medical, educational, employment*, dan yang lainnya. Data ini dikumpulkan sebelum proses komputerisasi, dan data privasi ini harus dilindungi. Agar hak-hak privasinya terjaga.

8. *Controlled of Evolution of Computer Use*

Konflik, satu sisi komputer digunakan untuk hal-hal yang berguna, tapi di sisi lain komputer digunakan untuk pengendalian nuklir yang mungkin saja digunakan untuk hal-hal yang tidak berguna.

E. Pendekatan Audit SI

Pesatnya perkembangan dunia komputer, diikuti dengan peningkatan pengetahuan auditor, ternyata mengundang dua perlakuan berbeda terhadap komputer, yaitu:

1. Komputer dipergunakan sebagai alat bantu auditor dalam melaksanakan audit, misalnya untuk mengambil contoh transaksi, memproses data akuntansi, mencetak surat konfirmasi piutang dan sebagainya.
2. Komputer dijadikan sebagai target audit, karena data di-*entry* ke komputer dan hasilnya dianalisis untuk menilai kehandalan pemrosesan dan keakuratan program komputer.

Dengan berjalannya evolusi tersebut, maka muncullah pendekatan audit sistem informasi yang dapat dikategorikan ke dalam tiga kelompok, yaitu:

a) *Auditing around the computer,* adalah mentrasir balik (*trace-back*) hasil olahan komputer antara lain output ke bukti dasarnya antara lain input tanpa melihat prosesnya.

b) *Auditing with the computer,* pendekatan ini menitikberatkan pada penggunaan komputer sebagai alat bantu audit. Alat bantu audit ini berupa komputer dilengkapi dengan software audit umum (*generale*

audit software, biasa disingkat GAS). Contoh GAS antara lain ACL (*Audit Command Language*), IDEA (*Interactive Data Extraction and Analysis*) dan lain-lain.

c) *Auditing throught the computer,* auditor harus memperlakukan komputer sebagai target audit dan melakukan audit *throught* atau memasuki area program. Oleh sebab itu, pendekatan *Auditing throught the computer* termasuk juga dalam CAATs (*Computer Assisted Audit Technique*) yaitu teknik audit berbantuan komputer (TABK).

Beberapa auditor memutuskan menggunakan pendekatan *Auditing throught* ini karena alasan berikut:

1) Ketidakmampuan untuk melokalisir *source document* atau *print-out* karena memang rancangan sistem pengarsipan yang digunakan menghendaki demikian.
2) Kekhawatiran bahwa jumlah yang ditunjukkan pada *print-out* komputer tidak sama dengan saldo yang ada (*ter-record*) di file komputer.

7

TAHAPAN AUDIT SISTEM INFORMASI

A. Tahapan Audit

Menurut Ron Weber dalam bukunya *Information Systems Control and Audit* halaman 47-55, terdapat 5 (lima) langkah atau tahapan audit sistem informasi, yaitu:

1. Perencanaan Audit (*Planning the Audits*)
2. Pengetesan Kendali (*Tests of Controls*)
3. Pengetesan Transaksi (*Tests of Transactions*)
4. Pengetesan Keseimbangan atau Keseluruhan Hasil (*Tests of Balances or Overall Results*) dan
5. Pengakhiran (penyelesaian) Audit (*Completion of the Audit*).

Sedangkan menurut Gallegos Cs. dalam bukunya *Audit and Control of Informtion Systems (chapter 10)*, tahapan audit sistem informasi mencakup aktivitas:

a) Perencanaan (*Planning*)
b) Pemeriksaan Lapangan (*Fieldwork*)
c) Pelaporan (*Reporting*) dan
d) Tindak Lanjut (*Follow Up*)

Planning adalah kegiatan perencanaan untuk melaksanakan audit, *Fieldwork* adalah kegiatan pemeriksaan dan evaluasi sistem yang dilaksanakan di lapangan, *Reporting* adalah kegiatan pelaporan hasil-hasil yang diperoleh dari *fieldwork* dan *Follow Up* adalah tindakan lebih lanjut yang dilaksanakan oleh pihak manajemen berkaitan dengan laporan hasil pemeriksaan.

B. Pengumpulan Fakta

Terdapat lima alat dan teknik yang dapat digunakan dalam mengumpulkan fakta, yaitu:

1. *Audit Software*: secara umum membahas audit software, audit khusus industri software, *high level language*, *utility software*, *expert systems*, *neural network software*, dan *software* lainnya.
2. *Code Review, Test Data, and Code Comparison*: secara umum membahas tentang di mana kesalahan (*error*) program terjadi dengan cara melihat kode program, tes data dan perbandingan kode.
3. *Concurrent Auditing Techniques*: membahas tentang teknik, kebutuhan dan implementasi untuk audit bersamaan. *Tipe concurrent auditing technique: integrated test facility, snapshort/extended record, system control/ audit review file, continous and intermittent simulation*.
4. *Interviews, Questionnaires, and Control Flowcharts*: membahas tentang desain dan penggunaan *interview*, kuisioner dan arus pengendalian.

   Wawancara (*Interviews*), digunakan untuk memperoleh baik jumlah (*quantitative*) maupun kualitas (*quality*) informasi selama pekerjaan pengumpulan fakta.

   Terdiri dari tiga fase, yaitu:

   a) persiapan wawancara (*preparing for interview*);
   b) pelaksanaan wawancara (*conducting the interview*) dan
   c) penganalisisan hasil wawancara (*analyzing the interview*).

   Kuesioner (*Questionnaires*), digunakan untuk mengumpulkan fakta berdasarkan data, seperti apakah ada pengendalian dalam sistem aplikasi.

Empat fase kuesioner, yaitu:

(1) desain pertanyaan (*design of questions*);

(2) desain skala respons (*design of response scales*);

(3) desain struktur dan layout (*design of the layout and structure*) dan

(4) jaminan bahwa kuesioner valid dan dapat dipercaya *(ensuring the questionnaire is valid and reliable)*.

Arus Pengendalian (*Control Flowcharts*), digunakan untuk menggambarkan apakah ada pengendalian dalam sistem dan di mana pengendalian itu berada dalam sistem.

5. *Performance Monitoring Tools,* mendiskusikan tentang objek dari pengukuran kinerja, karakteristik dari pengawasan pengukuran, *hardware, software, firmware*, dan pengawasan pengukuran campuran (*hybrid*), bagaimana hasil dari pengukuran kinerja, dan risiko untuk pemeliharaan integritas data sewaktu pengawasan kinerja dilakukan

[Halaman ini sengaja dikosongkan]

8

COBIT DAN PEDOMAN AUDIT

A. Pendahuluan

Pedoman audit menyediakan alat yang saling melengkapi untuk memungkinkan aplikasi yang mudah dari kerangka kerja COBIT dan tujuan-tujuan pengendalian dalam audit dan kegiatan penilaian. Maksud pedoman audit adalah untuk menyediakan struktur yang sederhana untuk mengaudit dan menilai pengendalian berdasarkan pada praktik audit yang diterima secara umum yang sesuai dengan skema COBIT keseluruhan. Pedoman audit ini menyediakan petunjuk untuk mempersiapkan perencanaan audit yang diintegrasikan dengan kerangka kerja COBIT dan tujuan pengendalian rinci, yang dapat dikembangkan ke dalam program audit khusus. Pedoman audit COBIT memungkinkan auditor me-*review* proses khusus TI terhadap tujuan pengendalian yang direkomendasikan, untuk membantu menjamin manajemen terhadap pengendalian yang memadai, atau memberi saran kepada manajemen apakah proses perlu ditingkatkan.

B. Kebutuhan Proses Bisnis

Untuk menetapkan bidang audit yang benar, dibutuhkan investigasi, analisis dan definisi:

1. proses bisnis yang bersangkutan.
2. platform dan sistem informasi yang mendukung proses bisnisnya juga antarkonektivitas dengan platform dan sistem lainnya.
3. peran dan tanggung jawab TI yang ditetapkan, termasuk yang telah menjadi sumber dalam dan luar.
4. risiko bisnis terkait dan pilihan strategis.

Langkah selanjutnya adalah mengidentifikasikan kebutuhan informasi yang ada relevansinya dengan proses bisnis. Selanjutnya diperlukan identifikasi risiko TI yang melekat juga tingkat pengendalian keseluruhan yang dapat diasosiasikan dengan proses bisnis, yakni:

a) perubahan yang ada dalam lingkungan bisnis yang berdampak pada TI.
b) perubahan yang ada pada lingkungan TI, perkembangan baru dan lain-lain.
c) kejadian yang ada, relevan terhadap pengendalian dan lingkungan bisnis.
d) pengendalian pemantauan TI diterapkan oleh manajemen.
e) audit yang ada dan atau laporan sertifikasi.
f) hasil yang ada pada penilaian itu sendiri.

Atas dasar informasi yang diperoleh, kita dapat menyeleksi proses COBIT yang relevan juga sumber daya yang dapat diterapkan. Selain itu harus menerapkan strategi audit atas dasar rencana audit rinci yang lebih lanjut harus diuraikan yakni dengan pendekatan berbasis pengendalian atau pendekatan substantif.

C. Pedoman Manajemen COBIT

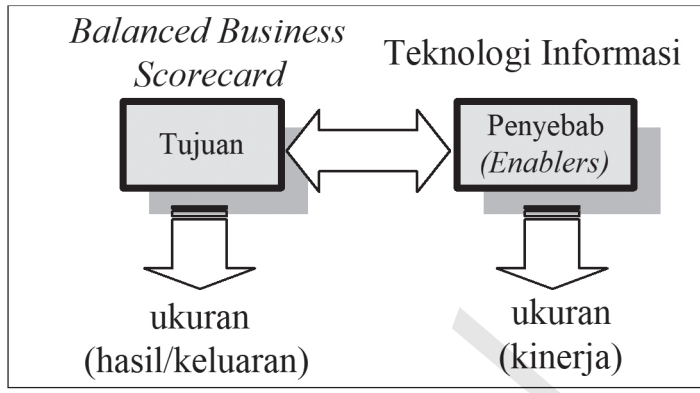
Institut IT Governance telah melakukan riset utama bekerja sama dengan kalangan akademisi, analis, dan para ahli dunia industri. Riset tersebut menghasilkan definisi pedoman manajemen untuk COBIT, yang terdiri dari model maturity, CSF, KGI, dan KPI, yang kemudian menyediakan manajemen dengan alat untuk menilai dan mengukur lingkungan TI organisasi terhadap 34 proses TI yang diidentifikasikan COBIT. Terdapat perubahan besar dalam TI dan jaringan yang menekankan informasi elektronik dan sistem TI untuk mendukung proses bisnis

kritis. Selanjutnya, bisnis yang sukses perlu pengaturan yang lebih baik dalam menghadapi teknologi yang komplek. Dengan meningkatnya pengungkapan kesalahan sistem informasi dan penyalahgunaan (*fraud*) elektronik, maka lingkungan organisasi memerlukan pengendalian yang teliti terhadap informasi. Saat ini manajemen TI terkait risiko tersebut dipahami sebagai bagian inti dari pengaturan perusahaan. Pengaturan TI yang merupakan bagian dari pengaturan perusahaan, menjadi lebih dirasakan peranannya dalam mencapai tujuan organisasi dengan menambah nilai melalui penyeimbangan risiko terhadap nilai kembali atas TI dan prosesnya. Pengaturan TI merupakan pelengkap suksesnya pengaturan perusahaan melalui peningkatan yang efisien dan efektif sehubungan dengan proses perusahaan. Pengaturan TI menyediakan stuktur yang berhubungan dengan proses TI, sumber daya TI, dan informasi untuk strategi dan tujuan perusahaan. Lebih lanjut, pengaturan TI mengintegrasikan dan melembagakan praktik yang berhubungan dengan PO, AI, DS, dan M kinerja TI untuk menjamin bahwa informasi perusahaan dan teknologi terkait mendukung tujuan bisnisnya. Selain itu pengaturan TI memungkinkan perusahaan mengambil keuntungan dari informasi tersebut.

Jawaban untuk kebutuhan penetapan ini dan pemantauan keamanan TI yang sesuai dan tingkat pengendalian adalah definisi dari:

a) *Benchmarking* praktik pengendalian TI (dinyatakan sebagai model *maturity*).
b) Indikator kinerja proses TI - untuk hasil dan kinerjanya.
c) CSF untuk mendapatkan proses dalam pengendalian ini.

Pedoman manajemen konsisten dan dibangun atas kerangka kerja COBIT, tujuan pengendalian dan pedoman audit. Selain itu, prinsip *balance business scorecard* digunakan untuk memfokuskan pada manajemen kinerja, yang membantu menetapkan KGI, mengidentifikasikan dan mengukur hasil proses dan KPI, menilai bagaimana proses dilaksanakan melalui ukuran yang memungkinkan. Oleh karena itu, hubungan antara tujuan bisnis dengan ukurannya dan TI dengan tujuan dan ukurannya sangat penting dan dapat digambarkan sebagai berikut:



Gambar 8.1 Hubungan Antara Tujuan dan Ukuran Bisnis dengan Tujuan dan Ukuran Ti [4]

Ukuran ini akan membantu manajemen dalam memantau organisasi dengan menjawab pertanyaan berikut:

1. Apa yang menjadi perhatian manajemen?

   Yakinkan bahwa kebutuhan perusahaan dipenuhi

2. Di mana diaturnya?

   Pada *Balanced Business Scorecard* sebagai *Key Goal Indicator* yang menggambarkan hasil proses bisnis.

3. Apa yang menjadi perhatian TI?

   Bahwa proses TI menyampaikan dasar informasi yang benar dan tepat pada perusahaan memungkinkan kebutuhan bisnis dipenuhi. Ini merupakan CSF bagi perusahaan.

4. Di mana diukurnya?

   Pada *Balanced Business Scorecard* TI, sebagai KGI yang menggambarkan hasil TI, dimana informasi tersebut disampaikan dengan kriteria yang benar (efektivitas, efisiensi, kerahasiaan, integritas, ketersediaan, pemenuhan dan keterandalan).

5. Kebutuhan-kebutuhan lain apa yang diukur?

   Apapun hasilnya secara positif dipengaruhi oleh sejumlah CSF yang perlu diukur sebagai KPI terhadap bagaimana TI berjalan dengan baik.

Model maturity untuk pengendalian terhadap proses TI terdiri dari pengembangan suatu metode penyusunan agar suatu organisasi dapat menilai tingkatan posisinya dari *non-existent* ke *optimised* (dari 0 sampai 5).

Pendekatan ini diambil dari *Maturity Model Software Engineering Institute* yang diterapkan untuk kematangan kemampuan pengembangan software. Terhadap tingkat ini, dikembangkan untuk setiap 34 proses TI COBIT, manajemen dapat menggambarkan:

a) status organisasi saat ini – di mana organisasi saat ini
b) status terbaik industri saat ini (di kelasnya) – sebagai perbandingan
c) status standar internasional saat ini – sebagai perbandingan
d) strategi organisasi untuk perbaikan atau peningkatan – ke arah mana keinginan organisasi

CSF menetapkan masalah terpenting atau tindakan untuk manajemen mencapai pengendalian proses TI. CSF harus mengatur orientasi pedoman implementasi dan mengidentifikasikan hal terpenting yang dilakukan secara strategis, teknis, organisasional atau prosedur.

KGI menetapkan ukuran yang mengarahkan manajemen setelah fakta – apakah proses TI telah mencapai kebutuhan bisnisnya, biasanya digambarkan atas kriteria informasi: ketersediaan informasi diperlukan untuk mendukung kebutuhan bisnis, ketiadaan atau kekurangan integritas dan risiko kerahasiaan, efisiensi biaya proses dan operasi, konfirmasi reliabilitas, efektivitas dan pemenuhan.

KPI menetapkan ukuran untuk menentukan bagaimana proses TI dilaksanakan dengan baik yang memungkinkan tujuan tersebut dicapai.

Secara ringkas dapat diuraikan sebagai berikut:

1) Model maturity, untuk pilihan strategis dan perbandingan *benchmarking*.
2) CSF, untuk mendapatkan proses dalam pengendalian.
3) KGI, untuk memantau pencapaian tujuan proses.
4) KPI, untuk memantau kinerja dalam setiap proses TI.

Kerangka kerja COBIT menetapkan 34 proses TI dalam lingkungan TI. Untuk setiap proses terdapat satu pertanyaan pengendalian tingkat tinggi dan antara 3 sampai 30 tujuan pengendalian rinci. Pemilik

proses harus dapat menetapkan tingkat yang melekat pada tujuan pengendalian. Untuk setiap 34 proses TI, terdapat skala ukuran naik, berdasarkan pada level 0-5, yang digambarkan dari "tidak ada *(Non Existent)*" sampai dengan "dioptimalisasi *(Optimised)*" sebagai berikut:

Tabel 8.1 Model Umum Maturity

Model Umum Maturity	
Level 0	Tidak ada ***(Non-Existent)***, kurang lengkapnya setiap proses yang dikenal. Organisasi belum mengenal adanya isu atau masalah yang diarahkan.
Level 1	Inisialisasi ***(Initial)***, ada bukti bahwa organisasi telah mengenal isu atau masalah yang ada dan perlu diarahkan. Tetapi tidak ada proses standardisasi, tetapi sekurang-kurangnya ada pendekatan khusus (*adhoc*) yang cenderung diterapkan pada individu atau dasar kasus demi kasus. Pendekatan terhadap keseluruhan manajemen tidak terorganisir.
Level 2	Dapat diulang ***(Repeatable)***, proses telah berkembang pada tahap di mana prosedur yang sama diikuti oleh orang yang berbeda dalam menjalankan tugas yang sama, tetapi tidak ada pelatihan formal atau prosedur komunikasi standar. Tanggung jawab diserahkan kepada setiap individu. Kepercayaan terhadap pengetahuan individu sangat tinggi sehingga seringkali terjadi kesalahan.
Level 3	Ditetapkan ***(Defined)***, prosedur telah distandarisasi dan didokumentasikan serta dikomunikasikan melalui pelatihan. tetapi imlementasinya masih bergantung pada individu apakah mau mengikuti prosedur tersebut atau tidak. Prosedur dikembangkan sebagai bentuk formalisasi dari praktik yang ada.
Level 4	Diatur ***(Managed)***, sudah memungkinkan untuk memantau dan mengukur ketaatan pada prosedur sehingga dapat dengan mudah diambil tindakan apabila proses yang ada tidak berjalan secara efektif. Perbaikan proses dilakukan secara tetap dan memberikan praktik terbaik. Otomasi dan peralatan yang digunakan terbatas.
Level 5	Dioptimalisasi ***(Optimised)***, proses telah disaring pada tingkat praktik terbaik berdasarkan pada hasil perbaikan yang terus menerus dan pengukuran model maturity dengan organisasi lain. TI digunakan dalam cara yang terintegrasi untuk mengotomatisasi arus kerja, menyediakan alat untuk meningkatkan kualitas dan efektivitas, membuat perusahaan mudah untuk beradaptasi.

a) Pengendalian

1) Definisi Pengendalian

Ron Weber (1999: 35) mengemukakan Pengendalian (*control*) adalah sebuah sistem yang digunakan untuk mencegah (*prevents*), mendeteksi (*detects*), atau mengkoreksi kejadian yang tidak dibenarkan (*unlawful events)*.

Tiga aspek kata kunci definisi pengendalian, yaitu:

i. Pengendalian adalah sebuah sistem *(a control is a system)*

   Dengan kata lain, terdiri dari sekumpulan komponen yang saling berelasi yang berfungsi secara bersama-sama untuk menyelesaikan suatu maksud atau tujuan.

ii. Kejadian yang tidak dibenarkan *(unlawful events)*

   Ketidakabsahan kegiatan dapat muncul jika tidak ada otorisasi *(unauthorized)*, tidak akurat *(inaccurate)*, tidak lengkap *(incomplete)*, redundansi *(redundant)*, tidak efektif *(ineffective)* atau tidak efisien *(inefficient)* pemasukan data ke dalam sistem.

iii. Ketiga, pemeriksaan digunakan untuk mencegah (*prevent)*, mendeteksi *(detect)*, atau mengoreksi *(correct)* kejadian yang tidak dibenarkan *(unlawful events)*.

2) Pendekatan Pengendalian

Dua pendekatan pengendalian, yaitu:

a) Pengendalian manajemen (*management control*), terdiri dari *Top Management Controls, Systems Development Management Controls, Programming Management Controls, Data Resource Management Controls, Security Management Controls, Operations Management Controls, dan Quality Assurance Management Controls*.

b) Pengendalian aplikasi (*application control*), terdiri dari, *Boundary Controls, Input Controls, Communication Controls, Processing Controls, Database Controls, dan Output Controls*.

Pengendalian terdiri dari dua jenis, yaitu pengendalian intern dan pengendalian ekstern. Pada kesempatan ini hanya akan dijelaskan mengenai pengendalian intern.

3) Definisi Pengendalian Internal

Definisi COBIT merujuk pada bagaimana COSO (*committee of sponsoring organization of the treadway commission*) mendefinisikan pengendalian sebagai serangkaian kebijakan, prosedur, praktik, dan struktur organisasi yang dirancang untuk menyiapkan keyakinan yang mendasar, bahwa tujuan organisasi atau perusahaan akan dapat dicapai dan hal-hal yang tidak dikehendaki akan terdeteksi atau terkoreksi. Di

samping itu, COBIT juga mengadaptasi definisi dari IT *contol objective* yang dikeluarkan oleh SAC (*system auditability and control*), yaitu suatu pernyataan tentang hasil yang dikehendaki atau direncanakan untuk dicapai dengan menerapkan prosedur-prosedur pengendalian di dalam kegiatan teknologi informasi yang terkait.

4) Tujuan Pengendalian Internal

Tujuan pengendalian TI didefinisikan sebagai suatu pernyataan hasil yang diinginkan atau maksud yang dicapai oleh prosedur pengendalian implementasi dalam kegiatan TI khusus.

Tujuan dari pengendalian internal adalah:

a) Memeriksa ketelitian dan kebenaran data yang akan menghasilkan laporan-laporan yang dapat diandalkan.
b) Efektivitas dan efisiensi dalam operasi, yaitu efektif dalam mencapai tujuan organisasi secara keseluruhan dan efisien dalam pemakaian sumber daya yang tersedia.
c) Membantu agar tidak terjadi penyimpangan terhadap hukum dan peraturan yang berlaku.
d) Mengamankan harta milik organisasi atau perusahaan termasuk data yang tersedia.

5) Klasifikasi Proses Pengendalian Sistem Informasi

COBIT *Framework* sebagaimana disebutkan dalam *IS Auditing Guidelines* pada bab *'Effect of Perfasive IS Control'* yang mulai berlaku efektif sejak 1 Maret 2000, membagi proses pengendalian sistem informasi ke dalam empat domain, yaitu:

a) Perencanaan dan pengorganisasian (PO: *Planning and Organisation*)
b) Akuisisi dan implementasi (AI: *Acquisition and Implementation*)
c) Penyampaian dan dukungan (DS: *Delivery and Support*)
d) Pemantauan (M: *Monitoring*)

Keempat domain tersebut di atas kemudian dijabarkan menjadi 34 faktor risiko yang harus dievaluasi jika ingin diperoleh suatu kesimpulan mengenai seberapa besar kepedulian manajemen terhadap teknologi informasi, serta bagaimana teknologi informasi dapat memenuhi kebutuhan manajemen akan informasi.

Tabel 6.2 Tiga Puluh Empat Faktor Risiko dan Pengendalian

***PLANNING AND ORGANISATION* (PO)**
1. PO1 Menetapkan Rencana Strategis Teknologi Informasi (*Define a Strategic IT Plan*)
2. PO2 Menetapkan Arsitektur Informasi (*Define the Information Architecture*)
3. PO3 Menetapkan Arah Teknologi (*Determine Technological Direction*)
4. PO4 Menetapkan Organisasi TI dan Hubungannya (*Define the IT Organisation and Relationships*)
5. PO5 Mengatur Investasi TI (*Manage the IT Investment*)
6. PO6 Mengomunikasikan Tujuan dan Arahan Manajemen (*Communicate Management Aims and Direction*)
7. PO7 Mengelola Sumber Daya Manusia (*Manage Human Resources*)
8. PO8 Memastikan Kesesuaian dengan Kebutuhan-kebutuhan eksternal (*Ensure Compliance with External Requirements*)
9. PO9 Menilai Risiko (*Assess Risks*)
10. PO10 Mengatur Proyek (*Manage Projects*)
11. PO11 Mengatur Kualitas (*Manage Quality*)
***ACQUISITION AND IMPLEMENTATION* (AI)**
12. AI1 Identifikasi solusi-solusi otomatisasi (*Identify Automated Solutions*)
13. AI2 Memperoleh dan memelihara Perangkat Lunak Aplikasi (*Acquire and Maintain Application Software*)
14. AI3 Memperoleh dan memelihara Infrastruktur Teknologi (*Acquire and Maintain Technology Infrastructure*)
15. AI4 Mengembangkan dan memelihara prosedur (*Develop and Maintain Procedures*)
16. AI5 Instalasi dan pengakuan sistem (*Install and Accredit Systems*)
17. AI6 Mengatur Perubahan (*Manage Changes*)
***DELIVERY AND SUPPORT* (DS)**
18. DS1 Menetapkan dan mengatur tingkatan pelayanan (*Define and Manage Service Levels*)
19. DS2 Mengelola layanan pihak ke tiga (*Manage Third-Party Services*)
20. DS3 Mengelola kapasitas dan kinerja (*Manage Performance and Capacity*)
21. DS4 Menjamin layanan berkelanjutan (*Ensure Continuous Service*)
22. DS5 Menjamin keamanan sistem (*Ensure Systems Security*)
23. DS6 Mengidentifikasikan dan mengalokasikan biaya (*Identify and Allocate Costs*)
24. DS7 Mendidik dan melatih user (*Educate and Train Users*)
25. DS8 Membantu dan memberikan masukan kepada pelanggan (*Assist and Advise Customers*)
26. DS9 Mengelola konfigurasi (*Manage the Configuration*)
27. DS10 Mengelola kegiatan dan permasalahan (*Manage Problems and Incidents*)
28. DS11 Mengelola Data (*Manage Data*)
29. DS12 Mengelola Fasilitas (*Manage Facilities*)
30. DS13 Mengelola Operasi (*Manage Operations*)

MONITORING (M)
31. M1 Mengawasi proses (*Monitor the Processes*) 32. M2 Menilai kecukupan pengendalian internal (*Assess Internal Control Adequacy*) 33. M3 Memperoleh jaminan independen (*Obtain Independent Assurance*) 34. M4 Menyediakan Audit Independen (*Provide for Independent Audit*)

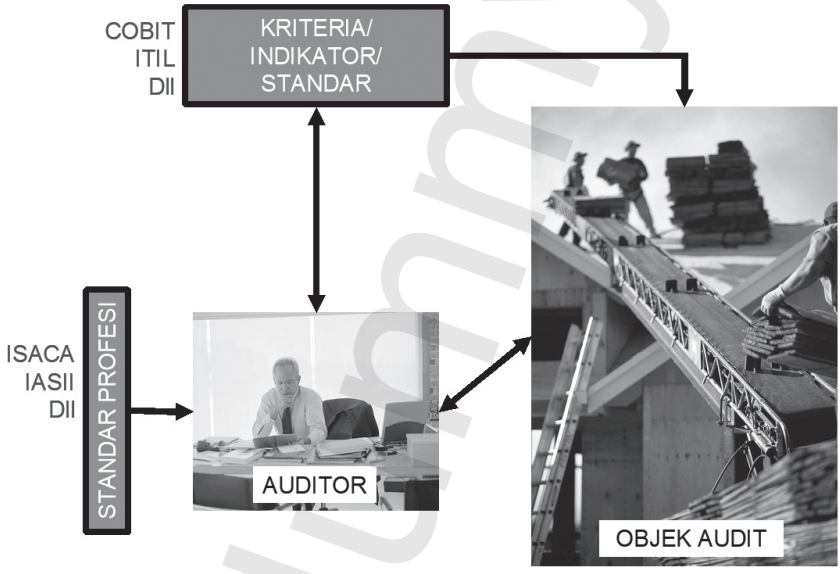
9

STANDAR PROFESI AUDIT SISTEM INFORMASI

A. Pendahuluan

Dalam praktik sehari-hari, sering menimbulkan salah persepsi antara pengertian "standar profesi audit sistem informasi" dan "standar audit sistem informasi". Kedua hal ini adalah dua hal yang berbeda. Standar profesi audit sistem informasi adalah standar yang diterbitkan oleh organisasi profesi audit sistem informasi. Standar profesi ini mengikat diri para anggota profesi tertentu. Standar profesi ini harus dijadikan acuan para anggota profesi dalam berinteraksi dengan pihak pemberi penugasan, objek yang diaudit, dan lingkungannya, baik selama proses audit ataupun setelah proses audit. Jika melanggar standar profesi ini, seorang anggota profesi dapat dikenakan sanksi oleh organisasinya, baik sanksi ringan berupa skorsing ataupun sanksi berat berupa pemecatan dari keanggotaan profesi. Di sisi lain, standar audit adalah "kriteria atau indikator" yang dijadikan dasar oleh seorang auditor sistem informasi dalam menilai suatu sistem informasi apakah sesuai dengan kriteria atau indikator yang telah ditentukan atau disepakati sebelumnya. Kriteria atau indikator ini biasanya diterbitkan oleh organisasi yang berwenang untuk dijadikan acuan oleh suatu perusahaan atau organisasi. Kriteria yang paling dikenal adalah Cobit dan *Information Technology Infrastructure Library* (ITIL). Kriteria ini belakangan dikenal sebagai tata kelola TI (IT *governance*). Implementasi kriteria atau indikator ini ada yang bersifat

wajib (*mandatory*) dan ada juga yang bersifat sukarela (*volunteer*). Sebagai contoh, Bank Indonesia dapat menerbitkan aturan mengenai sistem *back-up* bagi bank-bank di Indonesia. Aturan yang diterbitkan oleh Bank Indonesia ini bersifat *mandatory* untuk melindungi para nasabah dan kepercayaan masyarakat terhadap bank. Namun, bank-bank di Indonesia juga dapat mengikuti aturan pada Basel II. Hanya saja, implementasi Basel II tersebut bersifat sukarela karena aturan-aturan yang ada di Basel II belum wajib ditaati oleh bank-bank yang ada di Indonesia (kecuali beberapa bank asing). Secara jelas, perbedaan antara "standar profesi audit sistem informasi" dan "standar audit sistem informasi" tampak dalam gambar berikut.



Gambar 9.1 Perbedaan Standar Profesi Audit dan Standar Audit

Akan halnya acuan tata kelola TI untuk sektor publik, Menteri Komunikasi dan Informatika telah menerbitkan Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi Nasional dengan Keputusan Nomor 41/PER/MEN.KOMINFO/11/2007. Panduan Tata Kelola TIK Nasional diperuntukkan bagi seluruh instansi pemerintah di semua level, yaitu departemen atau LPND di tingkat pusat, provinsi, dan kabupaten/kota. Walaupun Panduan Tata Kelola TIK Nasional ini tidak mengatur pengelolaan TIK di badan usaha milik negara seperti BUMN

dan BUMD, Panduan ini juga bisa dijadikan acuan oleh badan usaha tersebut, termasuk badan usaha swasta. Sebab, salah satuan acuan dari penyusunan Panduan ini telah mengacu kepada international best practices, yaitu Cobit, ITIL, dan ISO 27000.

B. ISACA

IS Auditing Standard seperti yang dikutip dari ISACA merupakan panduan dasar bagi auditor sistem informasi agar dapat memenuhi tanggung jawab profesional mereka, seperti yang tercantum dalam "ISACA *Code of Profesional Ethics*" .

IS Auditing Standard terdiri dari:

1. Audit Charter
   a) Tujuan, pertanggungjawaban dan otoritas dari fungsi audit sistem informasi atau penugasan sistem informasi seharusnya didokumentasikan dengan baik dalam surat perjanjian
   b) Surat perjanjian tersebut haruslah disetujui oleh manajemen level atas organisasi.
2. *Independence*
   a) Profesional Independence. Dalam kondisi apa pun yang berkaitan dengan audit, auditor sistem informasi harus dapat independent, baik dalam mengaudit maupun penampilannya.
   b) Organisational Independence. Fungsi audit sistem informasi harus independen terhadap area atau aktivitas yang akan dievaluasi untuk memenuhi tujuan dari penugasan audit.
3. *Profesional Ethics and Standards*. Auditor sistem informasi harus setia terhadap etika profesional ISACA dalam menjalani tugasnya.
4. *Profesional Competence*
   a) Auditor sistem informasi haruslah memiliki keterampilan maupun pengetahuan yang cukup dalam menjalani tugasnya.
   b) Auditor sistem informasi haruslah senantiasa mempertahankan kemampuan profesional mereka melalui pelatihan dan pembelajaran secara rutin dan berkelanjutan.

5. *Planning*
    a) Auditor sistem informasi harus mengembangkan dan melakukan pendokumentasian terhadap pendekatan audit berbasis risiko (*risk-based audit approach*).
    b) Auditor sistem informasi haruslah dapat mengembangkan program audit untuk mencapai tujuan akhir dalam pelaksanaan tugasnya.
6. *Performance of Audit Work*
    a) Staf audit sistem informasi haruslah berada dalam pengawasan untuk menyediakan jaminan bahwa tujuan audit terpenuhi dan standar profesional audit telah terpenuhi.
    b) Selama proses audit dilakukan, auditor harus memiliki bukti yang cukup, pantas, dan relevan.
    c) Proses audit haruslah didokumentasikan, untuk mengambarkan kinerja pekerjaan audit yang telah dilakukan.
7. *Reporting*
    a) Auditor sistem informasi harus menyediakan laporan. Laporan haruslah mengindentifikasikan organisasi, penerimanya, dan batasan-batasan dalam sirkulasinya.
    b) Auditor harus memiliki bukti yang cukup dan relevan untuk mendukung laporan tersebut.
    c) Ketika laporan diterbitkan, laporan haruslah ditandatangani dan distribusikan sesuai surat perjanjian di awal.
8. *Follow-up Activites*. Setelah melaporkan temuan dan rekomendasi, auditor sistem informasi harus meminta dan mengevaluasi informasi yang relevan untuk memastikan apakah tindakan yang benar telah diambil oleh manajemen.
9. *Irregularities and Illegal Acts*
    a) Dalam merencanakan dan melaksanakan audit untuk mengurangi risiko, auditor sistem informasi harus mempertimbangkan risiko dari tindakan penyalahgunaan dan pelanggaran hukum (*irregularities and illegal acts*).
    b) Auditor sistem informasi haruslah mendapatkan pengertian dari organisasi meliputi internal controlnya.

c) Auditor sistem informasi harus merancang dan menjalankan prosedur untuk menguji kepantasan dari internal control.

d) Auditor sistem informasi harus mendokumentasikan semua komunikasi, rencana, hasil, evaluasi, dan keyakinan yang terkait dengan tindakan penyalahgunaan dan pelanggaran hukum yang telah dilaporkan kepada manajemen.

10. *IT Governance*

a) Auditor sistem informasi harus mengevaluasi dan menaksir apakah fungsi sistem informasi sejalan dengan misi, visi, nilai, tujuan, dan strategi organisasi.

b) Auditor sistem informasi harus mengevaluasi apakah fungsi sistem informasi memiliki kejelasan mengenai kinerja yang diharapkan oleh bisnis.

c) Pendekatan risiko harus digunakan oleh auditor sistem informasi untuk mengevaluasi fungsi sistem informasi.

d) Auditor sistem informasi harus mengevaluasi dan menaksir *control environment* dari organisasi.

e) Auditor sistem informasi harus mengevaluasi dan menaksir risiko yang memiliki efek merugikan terhadap lingkungan sistem informasi.

11. *Use of Risk Assesment in Audit Planning*

a) Auditor sistem informasi harus menggunakan teknik taksiran atau pendekatan risiko yang pantas dalam mengembangkan rencana audit dan menetapkan prioritas terhadap sumber daya sistem informasi.

b) Dalam merencanakan evaluasi individu, auditor sistem informasi harus mengindentifikasi dan menaksir risiko yang relevan terhadap area yang dievaluasi.

12. *Audit Materiality*

a) Dalam merencanakan proses audit, auditor harus mempertimbangkan kelemahan potensial akibat ketiadaan pengendalian.

b) Laporan auditor sistem informasi harus mengungkap ketidakefektifan pengendalian tersebut.

13. *Using the Work of Other Experts*
    a) Auditor jika memungkinkan, diperbolehkan mempertimbangkan menggunakan pekerjaan audit dari auditor lainnya.
    b) Auditor harus menambahkan test tambahan untuk memperoleh bukti audit, jika pekerjaan dari auditor lainnya tidak menyediakan bukti yang cukup.
14. *Audit Evidence*
    a) Auditor sistem informasi harus menyediakan bukti yang cukup dan pantas untuk menarik kesimpulan berdasarkan pada hasil audit.
    b) Auditor harus mengevaluasi kecukupan bukti audit yang didapat selama melakukan audit.
15. *IT Control*
    a) Auditor harus mengevaluasi dan memonitor pengendalian-pengendalian TI yang merupakan bagian integral dari lingkungan pengendalian internal suatu organisasi.
    b) Auditor harus membantu manajemen dengan memberikan nasihat mengenai rancangan, implementasi, operasi, dan peningkatan pengendalian-pengendalian TI.
16. *E-Commerce*. Auditor harus mengevaluasi pengendalian yang dapat diterapkan dan menilai risiko ketika menelaah pengendalian *e-commerce* untuk menjamin bahwa transaksi *e-commerce* dikendalikan dengan baik.

C. IASII

Standar Audit Sistem Informasi (SASI) juga diberlakukan di Indonesia. SASI di Indonesia dikeluarkan oleh Ikatan Audit Sistem Informasi Indonesia (IASII) yang dapat dijabarkan sebagai berikut:

1. Penugasan Audit

   Tanggung Jawab, Wewenang dan Akuntabilitas. Tanggung jawab, wewenang, dan akuntabilitas dari auditor sistem informasi harus dinyatakan dengan jelas secara formal dan tertulis dalam piagam atau surat tugas audit sistem informasi serta disetujui secara bersama oleh auditor sistem informasi dan pemberi tugas.

2. Independensi and Objektivitas
    a. Independensi. Dalam berbagai hal yang berkaitan dengan audit sistem informasi, auditor sistem informasi harus menjaga independensinya, baik secara faktual maupun penampilan, dari organisasi atau hal yang diaudit.
    b. Objektivitas. Auditor sistem informasi harus menjaga objektivitasnya dalam merencanakan, melaksanakan dan melaporkan audit sistem informasi.
3. Profesionalisme and Kompetensi
    a. Profesionalisme. Auditor sistem informasi harus memenuhi berbagai standar audit yang berlaku serta menerapkan kecermatan dan keterampilan profesionalnya dalam merencanakan, melaksanakan, dan melaporkan audit sistem informasi.
    b. Kompetensi. Auditor sistem informasi, secara kolektif, harus memiliki atau memperoleh pengetahuan dan keahlian yang diperlukan untuk melaksanakan audit sistem informasi.
    c. Pendidikan Profesi Berkelanjutan. Auditor sistem informasi harus meningkatkan pengetahuan dan keahlian yang diperlukan untuk melaksanakan audit sistem informasi melalui pendidikan profesi berkelanjutan.
4. Perencanaan.

    Perencanaan Audit. Auditor sistem informasi harus merencanakan audit sistem informasi dengan baik agar dapat mencapai tujuan audit serta memenuhi standar audit yang berlaku.
5. Pelaksanaan.
    a. Pengawasan. Staf audit sistem informasi harus disupervisi dengan baik untuk memberikan keyakinan yang memadai bahwa tujuan audit sistem informasi dapat tercapai dan standar audit yang berlaku dapat dipenuhi.
    b. Bukti-bukti Audit. Dalam melaksanakan audit sistem informasi, auditor sistem informasi harus memperoleh bukti-bukti audit yang cukup, dapat diandalkan dan bermanfaat untuk mencapai tujuan audit sistem informasi secara efektif. Temuan dan kesimpulan audit sistem informasi harus didukung oleh

analisis dan interpretasi yang memadai atas bukti-bukti audit tersebut.

c. Kertas Kerja Audit. Dalam melaksanakan audit sistem informasi, auditor sistem informasi harus mendokumentasikan secara sistematis seluruh bukti-bukti audit yang diperoleh serta analisis yang dilakukannya.

6. Pelaporan.

   Laporan Audit. Setelah menyelesaikan pelaksanaan audit sistem informasi, auditor sistem informasi harus memberikan suatu laporan audit sistem informasi dalam bentuk yang memadai kepada pihak-pihak yang berhak menerima. Laporan audit sistem informasi harus menyatakan lingkup, tujuan, sifat penugasan, temuan, kesimpulan, rekomendasi, identitas organisasi, penerima dan batasan distribusi laporan, serta batasan atau pengecualian yang berkaitan dengan pelaksanaan audit sistem informasi.

7. Tindak Lanjut.

   Pemantauan Tindak Lanjut. Auditor sistem informasi harus meminta dan mengevaluasi informasi yang dipandang perlu sehubungan dengan temuan, kesimpulan dan rekomendasi audit yang terkait dari audit sebelumnya untuk menentukan apakah tindak lanjut yang layak telah dilaksanakan dengan tepat waktu.

D. Acuan Tata Kelola di Indonesia

Istilah tata kelola atau *"governance"*, yang menggantikan *"government"* kembali berkembang pada tahun 1990, setelah munculnya reformasi administrasi publik melalui *National Performance Review* dan gerakan *reinventing government* di Amerika Serikat. Istilah ini kemudian berkembang di perusahaan publik menjadi *good corporate governance*. Setelah itu, istilah ini juga dipopulerkan pada dunia TI, yaitu *IT governance*, yang membedakannya dengan *IT management*. Istilah ini di Indonesia lebih sering diterjemahkan sebagai tata-kelola. Menurut Wessels dan Loggerenberg (2006), *"IT governance aims to align business and information technology strategies. Organizations adopt IT governance to ensure efficiency, decreased costs and increased control of IT infrastructures."* Beberapa pihak percaya bahwa *IT governance* akan meningkatkan akuntabilitas organisasi, yang pada akhir mengembalikan investasi. Kerangka kerja

(*framework*) IT governance seperti COBIT dan ITIL secara internasional telah diterima dan mempromosikan manfaat tersebut. Dengan memperhatikan bahwa penggunaan TI oleh institusi pemerintahan di Indonesia sudah dilakukan sejak beberapa dekade lalu, dengan intensitas yang semakin meningkat dan untuk memastikan penggunaan TI tersebut benar-benar mendukung tujuan penyelenggaraan pemerintahan, dengan memperhatikan efisiensi penggunaan sumber daya dan pengelolaan risiko terkait dengannya, Pemerintah Indonesia memandang perlu mengimplementasikan tata-kelola yang terkait dengan TIK, dengan menerbitkan Panduan Tata-kelola TIK Nasional melalui Keputusan Menteri Komunikasi dan Informatika Nomor 41/ PER/MEN.KOMINFO/11/2007. Panduan Tata-kelola TIK Nasional ini disusun dengan mengacu kepada:

a) COBIT (*Control Objective for Information and Related Technology*) versi 4.1
b) ITIL (*Information Technology Infrastructure Library*)
c) ISO 27000 (*Information Security Management System*)
d) AS 8015-2005 (*Australian Standard on Corporate Governance of Information & Communication Technology*)
e) Riset CISR MIT (*Center for Information System Research* – MIT) tentang IT Governance
f) Keppres 20 tahun 2006 tentang Dewan TIK Nasional
g) Keppres 80 tahun 2003 tentang Pedoman Pelaksanaan Pengadaan Barang/Jasa Pemerintah
h) PP No. 20 tahun 2004 tentang Rencana Kerja Pemerintah
i) PP No. 21 tahun 2004 tentang Penyusunan Rencana Kerja dan Anggaran Kementrian Negara/Lembaga
j) UU No. 32 tahun 2004 tentang Pemerintahan Daerah

Dalam panduan ini diuraikan mengenai (1) struktur dan peran tata-kelola dan (2) proses tata-kelola. Struktur dan peran tata-kelola adalah entitas apa saja yang berperan dalam pengelolaan proses-proses TI dan bagaimana pemetaan perannya dalam pengelolaan proses-proses TI tersebut. Struktur dan peran tata-kelola ini mendasari seluruh proses tata-kelola TIK. Proses tata-kelola adalah proses-proses yang ditujukan untuk memastikan bahwa tujuan-tujuan utama tata-kelola

dapat tercapai, terkait dengan pencapaian tujuan organisasi, pengelolaan sumber daya, dan manajemen risiko.

Proses tata-kelola dibagi dalam lingkup proses tata-kelola dan mekanisme proses tata-kelola. Lingkup proses tata-kelola terdiri dari:

a) Perencanaan Sistem, yaitu proses yang menangani identifikasi kebutuhan organisasi dan formulasi inisiatif-inisiatif TI apa saja yang dapat memenuhi kebutuhan organisasi tersebut.
b) Manajemen Belanja/Investasi, yaitu proses yang menangani pengelolaan investasi/belanja TI
c) Realisasi Sistem, yaitu proses yang menangani pemilihan, penetapan, pengembangan/akuisisi sistem TIK, serta manajemen proyek TIK.
d) Pengoperasian Sistem, yaitu proses yang menangani operasi TI yang memberikan jaminan tingkat layanan dan keamanan sistem TI yang dioperasikan.
e) Pemeliharaan Sistem, yaitu proses yang menangani pemeliharaan aset-aset TI untuk mendukung pengoperasian sistem yang optimal

Mekanisme proses tata-kelola terdiri dari:

a) Kebijakan Umum, yaitu kebijakan umum yang ditetapkan untuk memberikan tujuan dan batasan-batasan atas proses TI bagaimana sebuah proses TI dilakukan untuk memenuhi kebijakan yang ditetapkan.
b) Monitoring dan Evaluasi, yaitu monitoring dan evaluasi yang ditetapkan untuk memastikan adanya umpan balik atas pengelolaan TIK, yaitu berupa ketercapaian kinerja yang diharapkan. Untuk mendapatkan deskripsi kinerja setiap proses TI digunakan indikator keberhasilan. Indikator keberhasilan inilah yang akan dapat digunakan oleh manajemen atau auditor, untuk mengetahui apakah proses TI telah dilakukan dengan baik.

E. Struktur dan Peran Tata-kelola

Penetapan entitas struktur tata-kelola ini dimaksudkan untuk memastikan kapasitas kepemimpinan yang memadai, dan hubungan antar satuan kerja/institusi pemerintahan yang sinergis dalam

perencanaan, penganggaran, realisasi sistem TIK, operasi sistem TIK, dan evaluasi secara umum implementasi TI di pemerintahan.

Berikut ini adalah ketentuan umum terkait dengan Struktur Tata-kelola.

1. Ketentuan struktur tata-kelola terkait dengan kepemimpinan:
    a) Untuk memastikan kapasitas kepemimpinan pengelolaan TI di semua level pemerintahan, setiap institusi pemerintahan harus menetapkan *Chief Information Officer* (CIO). CIO ini bertugas mengoordinasi perencanaan, realisasi, operasional harian dan evaluasi internal TI di institusinya masing-masing, bekerja sama dengan satuan kerja TI dan satuan kerja pengguna lainnya.
    b) Puncak dari hierarki struktur tata-kelola terkait dengan kepemimpinan ini adalah keberadaan CIO Nasional yang bertugas mengoordinasi perencanaan, realisasi, operasional dan evaluasi TI khususnya terkait dengan flagship-flagship nasional TI prioritas.
2. Ketentuan struktur tata-kelola terkait dengan hubungan sinergis antarsatuan kerja dalam satu institusi atau hubungan sinergis antar-institusi:
    a) Untuk memastikan hubungan sinergis antarsatuan kerja dalam satu institusi pemerintahan dalam pengelolaan inisiatif TIK, setiap institusi pemerintahan harus membentuk Komite TIK. Komite TI ini mewadahi kepentingan satuan kerja TI dan satuan kerja-satuan kerja pengguna TIK, mengoordinasikan perencanaan dan operasional inisiatif-inisiatif TI strategis institusi pemerintahan terkait.
    b) Puncak dari hierarki struktur tata-kelola terkait dengan hubungan sinergis antar-institusi pemerintahan ini adalah keberadaan Dewan TI Nasional. Dewan TI Nasional ini bertugas memastikan implementasi TI yang tepat dan berkelanjutan secara nasional, dan secara khusus juga mengoordinasikan hubungan antar-institusi pemerintahan di tingkat departemen/LPND untuk memastikan terlaksananya flagship-flagship TI nasional prioritas.

Pembentukan CIO dan Komite TI di tiap institusi pemerintahan merupakan prioritas, disamping entitas-entitas struktur tata-kelola TI yang sudah ada sebelumnya:

1) Eksekutif Institusi Pemerintahan, yaitu pimpinan institusi pemerintahan (Kabupaten/Kota, Provinsi, Departemen, LPND).
2) Satuan Kerja Pengelola TIK, yaitu satuan kerja yang bertugas dalam pengelolaan TI institusi pemerintahan. Posisi struktural satuan kerja pengelola TI ini saat ini mempunyai level struktural yang berbeda-beda di institusi-institusi pemerintahan.
3) Satuan Pemilik Proses Bisnis, yaitu satuan kerja di luar satuan kerja pengelola TI sebagai pemilik proses bisnis (*business process owner*).

Peran-peran yang mempunyai kaitan langsung dengan mekanisme tata-kelola TI nasional adalah sebagai berikut:

1. Dewan TI Nasional:
   a) Bertanggung jawab atas sinkronisasi dan integrasi Rencana TI Nasional, khususnya di level departemen/lembaga tingkat pusat.
   b) Melakukan *review* atas rencana belanja/investasi TI departemen/lembaga tingkat pusat untuk memastikan tidak terjadinya tumpang tindih (*redundancy*) inisiatif TIK.
   c) Mendorong terwujudnya tata-kelola TI yang baik di seluruh institusi pemerintahan.
2. CIO Nasional:
   a) Memfasilitasi perencanaan dan implementasi insiatif TI lintas departemen/lembaga di tingkat pusat, khususnya flagship nasional.
   b) Memfasilitasi tata-kelola TI yang baik di seluruh institusi pemerintahan melalui penerbitan: kebijakan, standar, prosedur, atau panduan yang relevan.
3. Eksekutif Institusi:
   a) Bertanggung jawab atas seluruh implementasi TI di institusinya.
   b) Bertanggung jawab atas arahan strategis dan evaluasi keseluruhan dari inisiatif TI di institusinya.

4. CIO Institusi:
    a) Mengoordinasi perencanaan dan pelaksanaan inisiatif dan portofolio TI institusi.
    b) Melakukan *review* berkala atas pelaksanaan implementasi TI di institusinya.
5. Komite TI Institusi:
    a) Mensinergiskan dan mengintegrasikan Rencana TI institusi yang mengakomodir kepentingan seluruh satuan kerja.
    b) Mensinergiskan rencana belanja/investasi satuan kerja untuk memastikan tidak adanya tumpang tindih (*redundancy*) inisiatif TIK.
    c) Melakukan *review* atas evaluasi berkala implementasi TI yang dilakukan oleh CIO, untuk memastikan keselarasan dengan rencana semula.
6. Satuan Kerja Pengelola TI Institusi:
    a) Bertanggung jawab atas implementasi sistem TIK, sesuai dengan spesifikasi kebutuhan yang diberikan oleh Satuan Kerja Pemilik Proses Bisnis.
    b) Bertanggung jawab atas keberlangsungan dan kualitas aspek teknis sistem TI dalam tahap operasional.
    c) Bertanggung jawab atas pemeliharaan aset-aset TI institusi.
7. Satuan Kerja Pemilik Proses Bisnis Institusi:
    a) Bertanggung jawab atas pendefinisian kebutuhan (*requirements*) dalam implementasi inisiatif TIK.
    b) Memberikan masukan atas implementasi TIK, khususnya kualitas operasional sistem TIK.

[Halaman ini sengaja dikosongkan]

10

LINGKUP PROSES TATA KELOLA

A. Perencanaan Sistem

Perencanaan sistem merupakan proses yang ditujukan untuk menetapkan visi, arsitektur TI dalam hubungannya dengan kebutuhan organisasi dan rencana realisasi atas implementasi visi dan arsitektur TI tersebut. Rencana TI yang telah disusun akan menjadi referensi bersama bagi seluruh satuan kerja dalam sebuah institusi atau referensi bersama beberapa institusi yang ingin mensinergiskan inisiatif TIK-nya. Sinkronisasi dan integrasi perencanaan sistem dilakukan sejak di level internal institusi maupun hubungan antarinstitusi. Komite TI institusi memberikan persetujuan akhir atas Rencana Induk TI lima tahunan institusi, yang kemudian akan disahkan secara legal dan formal oleh eksekutif institusi. Dewan TI Nasional melakukan review dan memberikan masukan atas perencanaan TI departemen atau lembaga di tingkat pusat.

Dewan TI Nasional memberikan persetujuan akhir atas Rencana Flagship Nasional, yang kemudian akan disahkan secara legal dan formal oleh eksekutif pemerintahan.Setiap institusi pemerintahan memiliki Rencana Induk TI lima tahunan yang akan menjadi dasar dalam pelaksanaan inisiatif TI tahunan, dengan memperhatikan keselarasan dengan Rencana Flagship TI Nasional.

Setiap institusi pemerintahan minimal harus memiliki perencanaan atas komponen berikut ini:

1. Arsitektur Informasi, yaitu model informasi organisasi yang mendefinisikan lingkup kebutuhan informasi yang dipetakan ke dalam proses bisnis organisasi terkait.
2. Arsitektur Aplikasi, yaitu model aplikasi organisasi yang mendefinisikan lingkup aplikasi beserta persyaratan dan spesifikasi desain apa saja yang dibutuhkan oleh organisasi untuk mengakomodasi seluruh level proses bisnis organisasi seperti: transaksional, operasional, pelaporan, analisis, monitoring dan perencanaan.
3. Arsitektur Infrastruktur Teknologi, yaitu: topologi, konfigurasi, dan spesifikasi infrastruktur teknologi beserta pendekatan siklus hidupnya untuk memastikan infrastruktur teknologi yang digunakan organisasi selalu sesuai dengan kebutuhan.
4. Organisasi dan Manajemen, yaitu struktur organisasi dan deskripsi peran, serta kebijakan dan prosedur untuk menjalankan seluruh proses dalam manajemen TIK.
5. Pendekatan dan Roadmap Implementasi, yaitu pola pendekatan yang digunakan untuk memastikan implementasi seluruh arsitektur beserta organisasi dan manajemen, didukung oleh roadmap implementasi yang mendeskripsikan tahapan-tahapan target implementasi dalam sebuah durasi waktu tertentu.

Komite TI institusi dapat melakukan review kekinian dan kesesuaian Rencana Induk TI institusi secara reguler.

a) Perencanaan Arsitektur Informasi

Tujuan yang ingin dicapai dengan perencanaan arsitektur informasi adalah tersedianya satu referensi model informasi organisasi, yang akan menjadi rujukan seluruh desain software aplikasi di tahap selanjutnya, dalam rangka mengurangi tingkat redundansi informasi. Arsitektur informasi mencakup informasi terstruktur (data mart, database, database tabel, pertukaran data) dan informasi tidak terstruktur (gambar, video, *file* dokumen, dan sejenisnya). Penetapan arsitektur informasi mencakup penetapan klasifikasi ke dalam kelas-kelas data, pemetaan kepemilikan data, dan

pendefinisian data *dictionary*, dan *syntax rules*. Arsitektur informasi juga menetapkan klasifikasi level keamanan data untuk setiap klasifikasi kelas data melalui penetapan kriteria yang tepat sesuai dengan kebutuhan organisasi.

b) Perencanaan Arsitektur Aplikasi

Tujuan yang ingin dicapai dengan perencanaan arsitektur aplikasi adalah terealisasinya dukungan atas proses bisnis di mana setiap aplikasi selalu akan berkorelasi terhadap sebuah proses bisnis tertentu yang didukungnya. Arsitektur aplikasi memberikan peta tentang aplikasi apa saja yang dibutuhkan sesuai dengan karakteristik konteks organisasi dan manajemen.

Secara umum kategorisasi dapat dilakukan atas:

1. Pelayanan Publik – merupakan aplikasi yang dikhususkan untuk memberikan pelayanan kepada warga dan komunitas bisnis, baik layanan informasi, komunikasi maupun transaksi.
2. Manajemen Internal – merupakan aplikasi yang dikhususkan untuk mengelola proses bisnis standar manajemen seperti keuangan, kepegawaian, pengelolaan aset, pengelolaan program kerja, monitoring kinerja, dan sejenisnya.
3. Pendukung Manajemen – merupakan aplikasi yang sifatnya mendukung operasional manajemen sehingga proses-proses bisnis standar manajemen dan pelayanan kepada publik dapat optimal, mencakup di antaranya fungsional informasi, komunikasi dan kolaborasi.
4. Data *warehouse & Business Intelligence* – merupakan aplikasi yang digunakan untuk mengelola laporan dan fasilitas analisis data multidimensional.

Efisiensi arsitektur teknis aplikasi ditempuh melalui pendekatan "One Stop Window" untuk setiap tipe pelanggan institusi pemerintah, terutama publik dan bisnis. Melalui pendekatan ini, publik hanya perlu mengakses satu sistem (menggunakan beragam *delivery channel*) untuk mendapatkan layanan TIK. Pendekatan ini terutama diimplementasikan untuk implementasi *egovernment* di lembaga/LPND, propinsi dan kabupaten/kota.

c) Perencanaan Arsitektur Infrastruktur Teknologi

Infrastruktur teknologi mencakup jaringan komunikasi, perangkat pemrosesan informasi (server, *workstation* dan peripheral pendukungnya), software system (sistem operasi, database RDBMS), dan media penyimpanan data. Perencanaan arsitektur infrastruktur teknologi diharapkan dapat mengutamakan mekanisme shared-services, fokus ini ditujukan untuk meningkatkan efisiensi belanja TIK. Mekanisme Shared-Services arsitektur teknis diimplementasikan atas aspek-aspek sumber daya berikut ini:

1) Infrastruktur komunikasi: jaringan komputer/komunikasi, koneksi internet.
2) Infrastruktur penyimpanan data (Data Center) dan/atau DRC (Disaster Recovery Center).

d) Perencanaan Manajemen dan Organisasi

Perencanaan organisasi mencakup identifikasi struktur organisasi pengelola yang akan melakukan operasional harian. Perencanaan manajemen mencakup pendefinisian prosedur teknis dengan prioritas pada domain:

1) Realisasi Sistem
2) Operasi Sistem
3) Pemeliharaan Sistem

e) Perencanaan Pendekatan dan Roadmap Implementasi

Setiap perencanaan sistem menyertakan skenario *project governance* untuk setiap proyek inisiatif TI yang direncanakan, untuk memastikan proyek-proyek inisiatif TI dapat diselesaikan tepat waktu, tepat sasaran, dan tepat anggaran. Setiap inisiatif yang direncanakan selalu menyertakan proyeksi waktu, kapan benefit yang diharapkan dapat terealisasi (*benefit realization schedule*). Setiap perencanaan sistem mempunyai roadmap implementasi yang didasarkan pada analisis kesenjangan arsitektur (informasi, aplikasi dan infrastruktur teknologi) serta kesenjangan manajemen dan organisasi. Roadmap implementasi terdiri dari portofolio program implementasi (yang dapat terdiri dari beberapa portofolio proyek untuk setiap programnya), penetapan peringkat prioritas portofolio proyek, dan pemetaan dalam domain waktu sesuai dengan durasi

waktu yang ditargetkan. Penetapan peringkat prioritas portofolio proyek inisiatif TI dilakukan setidaknya berdasarkan faktor level anggaran yang dibutuhkan, kompleksitas sistem, dan besar usaha yang diperlukan. Indikator keberhasilan proses ini adalah keselarasan strategis dan efisiensi arsitektur teknis. Keselarasan strategis ditandai oleh (1) tingkat konsistensi dengan Rencana TI Nasional; (2) tingkat kontribusi tujuan TI dalam mendukung tujuan organisasi secara umum, dalam perspektif desain; (3) tingkat kepuasan *stakeholders* atas Rencana TI yang sudah disusun, dalam perspektif akomodasi kepentingan; dan (4) tingkat kesesuaian proyek-proyek TI yang sudah/sedang berjalan dibandingkan dengan yang direncanakan; kesahihan dasar pengambilan keputusan jika terjadi deviasi khususnya untuk proyek-proyek TI yang kritikal/ strategis. Efisiensi arsitektur teknis ditandai oleh penurunan tingkat redundansi sistem akibat kurang optimalnya implementasi mekanisme shared-services arsitektur teknis.

B. Manajemen Belanja/Investasi

Manajemen Belanja/Investasi TI merupakan proses pengelolaan anggaran untuk keperluan belanja/investasi TIK, sesuai dengan mekanisme proyek inisiatif TI yang telah ditetapkan sebelumnya dalam Portotolio Proyek Inisiatif TI dan Roadmap Implementasi. Realisasi belanja/investasi ini dilakukan melalui mekanisme penganggaran tahunan. Pengelolaan belanja/investasi TI dilakukan melalui mekanisme penyusunan Rencana Kegiatan dan Anggaran institusi, seiring dengan bidang-bidang lainnya, sesuai dengan regulasi yang berlaku. Untuk level internal institusi, Komite TI Institusi melakukan review dan persetujuan atas Rencana Kegiatan dan Anggaran TI yang diajukan oleh Satuan Kerja Pengelola TI atau Satuan Kerja Pemilik Proses Bisnis. *Review* dan persetujuan ini ditujukan untuk memastikan tidak adanya redundansi proyek TI di tiap institusi. Dewan TI Nasional melakukan *review* dan memberikan persetujuan atas Rencana Kegiatan dan Anggaran TI departemen dan lembaga di tingkat pusat, serta Rencana Kegiatan dan Anggaran TI yang terkait langsung dengan implementasi Flagship TI Nasional. Ada dua tipe pengeluaran (*expenditures*) yang bisa muncul dalam anggaran belanja TIK, yaitu Pengeluaran Operasi (*Operational Expenditure* = OpEx) dan Pengeluaran Modal (*Capital Expenditure* =

CapEx). Pengeluaran Operasi (OpEx) TI adalah pengeluaran TI dalam rangka menjaga tingkat dan kualitas layanan. Yang bisa dimasukkan dalam kriteria OpEx adalah antara lain biaya gaji & lembur, biaya sewa alat, biaya overhead, ATK dan lain-lain. Pengeluaran modal (CapEx) TI adalah investasi dalam bentuk aset/infrastruktur TI yang diperlukan untuk memberikan, memperluas dan/atau meningkatkan kualitas layanan publik. Nilai buku aset akan disusut (depresiasi) selama umur ekonomisnya yang wajar (kecuali tanah). Yang termasuk CapEx antara lain: pembangunan/pembelian jaringan, server & PC, perangkat lunak, bangunan, dan tanah. Beberapa faktor yang mesti dipertimbangkan dalam pemilihan pola penganggaran CapEx dan OpEx, yaitu umur ekonomis sumber daya TIK, ketersediaan anggaran, tingkat kecepatan keusangan (absoleteness), nilai strategis TIK, karakteristik proyek, urgensi, ketersediaan pemasok, ketersediaan sumber daya, penganggaran modal, serta visi dan misi institusi.

1. Umur ekonomis sumber daya TIK

   Pengeluaran TI yang mempunyai umur ekonomis lebih dari satu tahun bisa dipertimbangkan untuk menggunakan CapEx.

2. Ketersediaan anggaran

   Jika institusi mempunyai anggaran TI yang terbatas sebaiknya menggunakan pola OpEx (misal sewa atau *outsourcing*) karena cenderung lebih murah dibanding beli atau buat sendiri.

3. Tingkat kecepatan keusangan (absoleteness)

   Untuk teknologi yang cepat usang dengan tingkat kembalian yang tidak jelas atau berjangka panjang maka sebaiknya menggunakan pola OpEx.

4. Nilai strategis TIK

   Sumber daya TI yang bernilai strategis tinggi (kerahasiaan, nilai ekonomi, kedaulatan negara, dan hal lain yang sejenis) sebaiknya menggunakan pola CapEx.

5. Karakteristik Proyek (skala, risiko, dan lain-lain)

   Proyek TI dengan skala (magnitude) besar biasanya juga punya risiko besar. Risiko yang besar bisa diminimalkan dengan menggunakan pola OpEx. Dengan OpEx, biaya dan risiko menjadi lebih terukur (bulanan atau tahunan).

6. Urgensi

   Sumber daya TI yang dibutuhkan ketersediaannya dalam waktu singkat bisa menggunakan OpEx, misal dengan cara sewa atau *outsourcing*.

7. Ketersediaan Pemasok

   Keberadaan pemasok (vendor) menjadi hal yang harus dipertimbangkan karena CapEx atau OpEx bisa tergantung dari ada tidaknya pemasok (vendor).

8. Ketersediaan Sumber Daya

   Sumber daya manusia TI yang ada di dalam institusi bisa menentukan pola yang akan digunakan. Jika institusi tidak memiliki SDM TI yang memadai maka OpEx (sewa atau *outsourcing*) bisa jadi pilihan.

9. *Capital Budgeting*

   Pembuatan keputusan belanja/investasi TI sebaiknya menggunakan perhitungan capital budgeting antara lain, *Internal Rate of Return* (IRR), *Net Present Value* (NPV), *Payback Period*, *Cost-Benefit Ratio*, dan *Return on Investment* (RoI).

10. Visi dan Misi Institusi

    Keputusan belanja/investasi TI bisa sangat dipengaruhi oleh visi dan misi institusi. Sebelum membuat keputusan belanja/investasi TI sebaiknya merujuk ke visi dan misi institusi untuk mengevaluasi relevansinya.

Indikator keberhasilan manajemen belanja/investasi antara lain:

1) Digunakannya sumber-sumber pendanaan yang efisien.
2) Kesesuaian realisasi penyerapan anggaran TI dengan realisasi pekerjaan yang direncanakan.
3) Diperolehnya sumber daya TI yang berkualitas dengan melalui proses belanja/investasi TI yang efisien, cepat, bersih dan transparan.

C. Realisasi Sistem

Realisasi sistem TI merupakan proses yang ditujukan untuk mengimplementasikan perencanaan TIK, mulai dari pemilihan sistem TI sampai dengan evaluasi pascaimplementasi.

1. Identifikasi dan Pemilihan Alternatif Sistem

   Pemilihan alternatif sistem atau proses pemilihan sistem dari alternatif sistem yang telah ada dilakukan dengan menggunakan referensi hasil studi kelayakan. Manajemen TI melakukan studi kelayakan yang setidaknya terdiri dari aktivitas:

   1) Penentuan kebutuhan secara fungsional proses bisnis dan persyaratan-persyaratan teknikal;
   2) Penentuan manfaat (benefit) apa yang hendak dicapai dengan keberadaan sistem yang akan dikembangkan; dan
   3) Analisis risiko terkait dengan proses bisnis

   Untuk sistem TI berskala besar, strategis, dan berpotensi mempengaruhi sistem-sistem TI sebelumnya, pemilihan alternatif sistem TI dapat dilakukan melalui mekanisme *proof of concept* (POC), di mana:

   a) Hanya sistem-sistem TI yang dinyatakan lulus POC yang dapat mengikuti proses formal seleksi atau tender; dan
   b) Pelaksanaan POC dilakukan berdasarkan skenario teknis yang disetujui oleh pihak institusi pemerintah dan vendor terkait.

   Pelaksanaan pemilihan sistem dari alternatif yang ada berdasarkan aturan terkait tentang pengadaan barang dan jasa yang sudah ada sebelumnya.

2. Realisasi Software Aplikasi

   Pengembangan dan/atau pengadaan (akuisisi) software aplikasi dilakukan berdasarkan metodologi *system development life cycle* (SDLC) yang dipergunakan secara luas oleh industri software, yang minimal mencakup kebutuhan akan:

   1) Penerjemahan kebutuhan/persyaratan bisnis ke dalam spesifikasi desain;
   2) Penyusunan desain detail dan teknikal software aplikasi, termasuk juga di sini pengendalian aplikasi (*application control*),

yang memungkinkan setiap pemrosesan dalam software apliasi akurat, lengkap, tepat waktu, terotorisasi dan dapat diaudit, dan pengendalian keamanan aplikasi (*application security control*), yang memungkinkan terpenuhinya aspek kerahasiaan (*confidentiality*), ketersediaan (*availability*), dan integritas (*integrity*);

3) Implementasi desain detail dan teknikal ke dalam kode program (*coding*);
4) Manajemen perubahan persyaratan/kebutuhan;
5) Pelaksanaan penjaminan mutu (*quality assurance*);
6) Uji-coba (*testing*), yaitu *unit testing*, *system testing*, *integration testing*, *user acceptance test* (UAT); dan
7) Instalasi dan akreditasi.

Metode SDLC juga diimplementasikan atas upgrade atas software aplikasi yang ada (*existing*) bersifat utama (*mayor*), yang menghasilkan perubahan signifikan atas desain dan fungsionalitas yang ada (*existing*).

Setiap software aplikasi yang direalisasikan harus disertai dengan *training* dan/atau transfer pengetahuan kepada pengguna dan administrator sistem.

Setiap software aplikasi yang direalisasikan harus disertai oleh dokumentasi berikut ini:

a) Dokumentasi hasil aktivitas tahapan-tahapan dalam SDLC;
b) Manual pengguna, operasi, dukungan teknis, dan administrasi; dan
c) Materi transfer pengetahuan dan materi training.

3. Realisasi Infrastruktur Teknologi

Teknologi infrastruktur mencakup perangkat keras pemrosesan informasi (server, *workstation*, dan peripheral), jaringan komunikasi dan software infrastruktur (sistem operasi, tool sistem).

Pertimbangan kapasitas infrastruktur teknologi disesuaikan dengan kebutuhan, sehingga setiap realisasi infrastruktur teknologi selalu disertai sebelumnya dengan analisis kebutuhan kapasitas.

Setiap realisasi infrastruktur teknologi selalu memperhatikan kontrol terkait dengan faktor keamanan dan auditability (memungkinkan audit atas kinerja dan sejarah transaksi yang dilakukan), dengan tingkat kedalaman spesifikasi disesuaikan dengan kebutuhan manajemen.

Tahapan testing selalu dilakukan sebelum masuk tahapan operasional, yang dilakukan di lingkungan terpisah (*environment test*) jika memungkinkan.

4. Realisasi Pengelolaan Data

   Setiap langkah pengelolaan data harus memperhatikan tahapan: input, proses, dan *output* data.

   Pada tahapan input, prosedur yang harus dijalankan adalah: prosedur akses data, prosedur transaksi data untuk memeriksa akurasi, kelengkapan, dan validitasnya, serta prosedur pencegahan kesalahan input data.

   Pada tahapan proses, prosedur yang harus dijalankan adalah: prosedur pengolahan data, prosedur validasi dan editing, serta prosedur penanganan kesalahan.

   Pada tahapan *output*, prosedur yang harus dijalankan adalah: prosedur distribusi, penanganan kesalahan, dan keamanan data.

   Indikator Keberhasilan dari proses ini adalah:

   a) Peningkatan jumlah realisasi sistem yang tidak mengalami backlog (tertunda dan mendesak untuk segera diselesaikan).
   b) Persentase realisasi sistem yang disetujui oleh pemilik proses bisnis dan manajemen TIK.
   c) Jumlah realisasi software aplikasi yang diselesaikan tepat waktu, sesuai spesifikasi dan selaras dengan arsitektur TIK.
   d) Jumlah realisasi software aplikasi tanpa permasalahan integrasi selama implementasi.
   e) Jumlah realisasi software aplikasi yang konsisten dengan perencanaan TI yang telah disetujui.
   f) Jumlah software aplikasi yang didukung dokumentasi memadai dari yang seharusnya.

g) Jumlah implementasi software aplikasi yang terlaksana tepat waktu.

h) Penurunan jumlah downtime infrastruktur.

D. Pengoperasian Sistem

Operasi sistem merupakan proses penyampaian layanan TIK, sebagai bagian dari dukungannya kepada proses bisnis manajemen, kepada pihak-pihak yang membutuhkan sesuai spesifikasi minimal yang telah ditentukan sebelumnya.

1. Manajemen Tingkat Layanan

   Manajemen TI bertanggung jawab atas penyusunan dan update katalog layanan TIK, yang berisi sistem yang beroperasi dan layanan-layanan TI yang menyusunnya. Diprioritaskan bagi layanan-layanan TI kritikal yang menyusun sebuah operasi sistem TI harus memenuhi (SLA) yang ditetapkan sebagai sebuah requirement (persyaratan) oleh pemilik proses bisnis dan disetujui oleh manajemen TIK. Aspek minimal yang harus tercakup dalam setiap SLA layanan TI kritikal tersebut mencakup:

   1) Waktu yang diperlukan untuk setiap layanan TI yang diterima oleh konsumen.
   2) Persentase tingkat ketersediaan (*availability*) sistem TIK.
   3) Waktu yang diperlukan untuk penyelesaian pengaduan insiden atau permasalahan dengan beberapa tingkatan kritikal sesuai dengan kebutuhan.

   Pencapaian SLA-SLA tersebut dilaporkan secara reguler oleh manajemen TI kepada Komite TI untuk di-*review*.

2. Keamanan dan Keberlangsungan Sistem

   Setiap operasi sistem TI harus memperhatikan persyaratan minimal aspek keamanan sistem dan keberlangsungan sistem, terutama sistem TI yang memfasilitasi layanan-layanan kritikal.

   Aspek keamanan dan keberlangsungan sistem minimal yang harus terpenuhi mencakup hal-hal berikut ini:

   a) *Confidentiality*: akses terhadap data/informasi dibatasi hanya bagi mereka yang punya otoritas.

b) *Integrity*: data tidak boleh diubah tanpa ijin dari yang berhak.

c) *Authentication*: untuk meyakinkan identitas pengguna sistem.

d) *Availability*: terkait dengan ketersediaan layanan, termasuk *up-time* dari situs web.

Mekanisme dasar yang harus dipenuhi untuk memastikan tercapainya aspek-aspek keamanan dan keberlangsungan sistem mencakup hal-hal berikut ini:

a) Untuk pengamanan dari sisi software aplikasi dapat diimplementasikan komponen standar (a) metode scripting software aplikasi yang aman; (b) implementasi mekanisme autentikasi dan otorisasi di dalam software aplikasi yang tepat; dan (c) pengaturan keamanan sistem database yang tepat.

b) Untuk pengamanan dari sisi infrastruktur teknologi dapat diimplementasikan komponen standar (a) *hardening* dari sisi sistem operasi; (b) *firewall*, sebagai pagar untuk menghadang ancaman dari luar sistem; (c) *Intrusion Detection System/ Intrution-Prevention Systems* (IDS/IPS), sebagai pendeteksi atau pencegah aktivitas ancaman terhadap sistem; (d) *Network monitoring tool*, sebagai usaha untuk melakukan monitoring atas aktivitas di dalam jaringan; dan (e) *Log processor & analysis*, untuk melakukan pendeteksian dan analisis kegiatan yang terjadi di sistem.

c) Untuk sistem kritikal dengan SLA yang ketat, dapat ditempuh melalui penyediaan sistem cadangan yang dapat secara cepat mengambil alih sistem utama jika terjadi gangguan ketersediaan (availability) pada sistem utama.

d) Assessment kerentanan keamanan sistem (*security vulnerability system*) secara teratur sesuai dengan kebutuhan.

e) Penyusunan IT Contingency Plan khususnya yang terkait dengan proses-proses bisnis kritikal, yang diuji validitasnya secara teratur sesuai dengan kebutuhan.

3. Manajemen Software Aplikasi

Setiap software aplikasi harus selalu menyertakan prosedur backup dan restore, dan juga mengimplementasikan fungsionalitasnya di

dalam software aplikasi. Setiap pengoperasian software aplikasi harus disertai oleh dokumentasi berikut ini:

1) Dokumentasi hasil aktivitas tahapan-tahapan dalam SDLC.
2) Manual Pengguna, Operasi, Dukungan Teknis dan Administrasi.
3) Materi transfer pengetahuan & Materi Training.

4. Manajemen Infrastruktur

   Setiap pengoperasian infrastruktur teknologi selalu memperhatikan kontrol yang terkait dengan faktor keamanan dan auditability (memungkinkan audit atas kinerja dan sejarah transaksi yang dilakukan).

5. Manajemen Data

   Data dari setiap software aplikasi secara kumulatif juga dibackup secara terpusat dalam media penyimpanan data (data storage), terutama software-software aplikasi kritikal.

   Backup data dilakukan secara reguler, dengan frekuensi dan jenis backup disesuaikan dengan tingkat kritikal sistem. Dilakukan pengujian secara teratur mekanisme backup dan restore data, untuk memastikan integritas dan validitas prosedur. Implementasi mekanisme inventori atas media-media penyimpanan data, terutama media-media yang *off-line*.

6. Manajemen Layanan oleh Pihak Ketiga

   Layanan TI dapat diselenggarakan sebagian atau seluruhnya oleh pihak ketiga, dengan mempertimbangkan faktor-faktor berikut ini:

   a) Sumber daya internal yang dimiliki oleh institusi pemerintah terkait kurang memungkinkan, untuk mencapai tingkat layanan minimal yang diberikan kepada konsumen (publik atau bisnis).
   b) Seluruh data yang diolah melalui layanan pihak ketiga adalah data milik institusi pemerintahan terkait, dan pihak ketiga harus menjaga kerahasiaannya dan tidak berhak menggunakannya untuk hal-hal di luar kerja sama dengan institusi pemerintahan.

   Seluruh layanan TI yang diselenggarakan oleh pihak ketiga harus mematuhi ketentuan-ketentuan operasi sistem yang telah dijelaskan sebelumnya:

a) Manajemen tingkat layanan.
b) Keamanan dan keberlangsungan sistem.
c) Manajemen Software Aplikasi.
d) Manajemen Infrastruktur.
e) Manajemen Data.

Secara reguler pihak ketiga penyelenggara layanan TI harus memberikan laporan atas tingkat kepatuhan terhadap ketentuan-ketentuan operasi sistem di atas.

Pihak institusi pemerintahan yang layanannya diselenggarakan oleh pihak ketiga terkait secara reguler dan insidental dapat melakukan audit atas laporan yang disampaikan oleh pihak ketiga untuk memastikan validitasnya, baik dilakukan secara internal atau menggunakan jasa pihak ketiga lain yang independen.

Indikator keberhasilan terkait dengan manajemen tingkat layanan adalah:

i. Prosentase operasi sistem kritikal yang layanan-layanan TIK-nya disertai dengan SLA
ii. Prosentase layanan TI yang memenuhi SLA Indikator Keberhasilan Terkait dengan keamanan dan keberlangsungan sistem
iii. Tingkat kepatuhan sistem terhadap kriteria minimum yang telah ditetapkan.
iv. Penurunan jumlah insiden yang terjadi terkait dengan permasalahan keamanan dan keberlangsungan sistem.
v. Penurunan jumlah insiden yang menyebabkan *downtime*.
vi. Penurunan jumlah waktu *downtime* total per durasi waktu.

Indikator keberhasilan terkait dengan manajemen software aplikasi adalah:

i. Tingkat kepatuhan pengguna terhadap prosedur-prosedur yang telah ditetapkan
ii. Penurunan jumlah kegagalan pengoperasian software aplikasi

Indikator keberhasilan terkait dengan manajemen infrastruktur adalah:

i. Tingkat kepatuhan pengguna terhadap prosedur-prosedur yang telah ditetapkan
ii. Penurunan jumlah kegagalan pengoperasian infrastruktur

Indikator keberhasilan terkait dengan manajemen data adalah:

i. Penurunan jumlah kegagalan restore data kritikal
ii. Penurunan jumlah insiden terkait dengan permasalahan integritas data.

Indikator keberhasilan terkait dengan manajemen layanan oleh pihak ketiga adalah:

i. Jumlah atau prosentase operasi sistem TI yang memenuhi SLA
ii. Jumlah atau prosentase operasi sistem TI yang memenuhi ketentuan minimum keamanan dan keberlangsungan sistem
iii. Jumlah atau prosentase operasi sistem TI yang memenuhi ketentuan minimum manajemen data
iv. Penurunan jumlah insiden yang menyebabkan *downtime*
v. Penurunan jumlah waktu *downtime* total per durasi waktu
vi. Penurunan jumlah kegagalan restore data kritikal
vii. Penurunan jumlah insiden terkait dengan permasalahan integritas data.

E. Pemeliharaan Sistem

Pemeliharaan sistem merupakan proses untuk memastikan bahwa seluruh sumber daya TI dapat berfungsi sebagaimana mestinya dalam durasi waktu siklus hidup yang seharusnya, dalam rangka mendukung operasi sistem secara optimal.

1. Pemeliharaan Software Aplikasi

   Manajemen TI menerapkan mekanisme patching software aplikasi atas software aplikasi yang dikembangkan secara mandiri atau kerjasama dengan pihak ketiga. Upgrade yang bersifat kecil (minor) atas software aplikasi minimal harus melalui regression test dan

harus disertai dengan update dokumentasi yang terkait langsung dengan modul yang diupgrade.

2. Pemeliharaan Infrastruktur Teknologi

   Manajemen TI menerapkan mekanisme patching infrastruktur teknologi (yaitu *update patch* atas infrastruktur teknologi untuk menutup lobang kerentanan) atas seluruh infrastruktur teknologinya. Mekanisme patching ini jika memungkinkan dapat difasilitasi secara otomatis dengan software tool, sehingga meningkatkan efisiensi di sisi administrator dan pengguna akhir. Mekanisme patching ini minimal dilakukan atas:

   1) System software Perangkat-perangkat jaringan
   2) System software di server dan workstation
   3) Database server

   Secara reguler manajemen TI melakukan penilaian pertumbuhan kapasitas dan membandingkannya dengan estimasi pertumbuhan. Berdasarkan analisis perbandingan tersebut, manajemen TI menyusun langkah untuk pengelolaan kapasitas dalam jangka menengah dan pendek.

3. Pemeliharaan Data

   Keaslian, keutuhan, dan ketersediaan data harus menjadi perhatian. Semua pihak dalam institusi harus menaati prosedur pemeliharaan data yang telah ditetapkan.

   Data Center/Disaster Recovery Center (DC/DRC) dikelola sesuai dengan prosedur baku yang ada.

   Data harus dilindungi dari pihak-pihak yang tidak memiliki hak akses serta pengubahan dan kesalahan alamat pengiriman data sensitif yang bernilai strategis.

4. Siklus Hidup dan Likuidasi Sumber Daya Infrastruktur Teknologi

   Siklus hidup infrastruktur teknologi yang diimplementasikan terdiri dari fasefase berikut:

   a) *Emerging technologies*, yaitu infrastruktur teknologi yang mungkin sudah diterima dan digunakan oleh industri terkait, tetapi masih baru bagi organisasi.

b) *Current technologies*, yaitu infrastruktur teknologi standar yang saat ini sedang digunakan oleh organisasi, telah dites dan diterima secara umum sebagai standar di industri terkait.

c) *Sunset technologies*, yaitu infrastruktur teknologi yang sudah masuk tahap phase-out (*expired*) dan sudah tidak dapat lagi digunakan oleh organisasi sejak waktu ditetapkan.

d) *Twilight technologies*, yaitu infrastruktur teknologi yang sudah masuk tahap phase-out (*expired*), tetapi masih diperlukan oleh organisasi.

Likuidasi sumber daya infrastruktur teknologi dapat dilakukan untuk infrastruktur teknologi di fase Sunset Technologies , dengan mempertimbangkan:

a) Sudah tidak adanya technical support.

b) Keberadaannya sudah dapat digantikan dengan kehadiran infrastruktur teknologi lain yang lebih handal dan terjangkau pengadaannya.

Likuidasi sumber daya infrastruktur teknologi diputuskan dalam pertemuan reguler Komite TIK.

Indikator Keberhasilan proses ini adalah:

i. Penurunan jumlah permasalahan yang terjadi di software aplikasi karena tidak optimalnya keberjalanan mekanisme patching

ii. Penurunan jumlah permasalahan yang terjadi di infrastruktur teknologi karena tidak optimalnya keberjalanan mekanisme patching

iii. Penurunan jumlah permasalahan yang terjadi karena aspek kapasitas infrastruktur teknologi

iv. Penurunan jumlah permasalahan yang terjadi karena aspek keutuhan (*integrity*), kerahasiaan (*confidentiality*), dan ketersediaan (*availability*) data.

v. Penurunan jumlah sumber daya infrastruktur teknologi di fase sunset yang masih belum dilikuidasi.

F. Mekanisme Proses Tata-kelola

Kebijakan umum merupakan pernyataan yang akan menjadi arahan dan batasan bagi setiap proses tata-kelola. Kebijakan ini berlaku untuk seluruh proses tata-kelola.

1. Keselarasan Strategis: Organisasi – TIK

   Arsitektur dan inisiatif TI harus selaras dengan visi dan tujuan organisasi. Keselarasan strategis antara organisasi – TI dicapai melalui mekanisme berikut:

   a) Keselarasan tujuan organisasi dengan tujuan TIK, di mana setiap tujuan TI harus mempunyai referensi tujuan organisasi.
   b) Keselarasan arsitektur bisnis organisasi dengan arsitektur TI (arsitektur informasi, arsitektur aplikasi, dan arsitektur infrastruktur).
   c) Keselarasan eksekusi inisiatif TI dengan rencana strategis organisasi.

Risiko-risiko prioritas dalam pengelolaan TI oleh institusi pemerintahan mencakup (1) risiko proyek, (2) risiko atas informasi, dan (3) risiko atas keberlangsungan layanan, di mana:

a) Risiko atas proyek mencakup kemungkinan tertundanya penyelesaian proyek TIK, biaya yang melebihi dari perkiraan atau hasil akhir (*deliverables*) proyek tidak sesuai dengan spesifikasi yang telah ditentukan di awal.
b) Risiko atas informasi mencakup akses yang tidak berhak atas aset informasi, pengubahan informasi oleh pihak yang tidak berhak dan penggunaan informasi oleh pihak yang tidak punya hak untuk keperluan yang tidak sebagaimana mestinya.
c) Risiko atas keberlangsungan layanan mencakup kemungkinan terganggunya ketersediaan (availabilitas) layanan TI atau layanan TI sama sekali tidak dapat berjalan.

Kontrol atas risiko proyek, risiko atas informasi, dan risiko atas keberlangsungan layanan secara umum mencakup:

1) Implementasi *Project Governance* untuk setiap proyek TI yang diimplementasikan oleh seluruh instansi pemerintahan.

2) Implementasi *Security Governance* di manajemen TI dan seluruh sistem TI yang berjalan, khususnya untuk meminimalkan risiko atas informasi dan keberlangsungan layanan.

Manajemen sumber daya dalam Tata-kelola TI ditujukan untuk mencapai efisiensi dan efektivitas penggunaan sumber daya TIK, yang melingkupi sumber daya: finansial, informasi, teknologi, dan SDM.

Ketercapaian efisiensi finansial dicapai melalui:

a) Pemilihan sumber-sumber dana yang tidak memberatkan untuk pengadaan TIK.
b) Kelayakan belanja TI secara finansial harus bisa diukur secara rasional dengan menggunakan metode-metode penganggaran modal (*capital budgeting*).
c) Dijalaninya prosedur pengadaan yang efisien dengan fokus tetap pada kualitas produk dan jasa TIK.
d) Prioritas anggaran diberikan untuk proyek TI yang bermanfaat untuk banyak pihak, berbiaya rendah, dan cepat dirasakan manfaatnya.
e) Perhitungan manfaat dan biaya harus memasukkan unsur-unsur yang bersifat kasat mata (*tangible*) dan terukur maupun yang tidak tampak (*intangible*) dan relatif tidak mudah diukur.
f) Efisiensi finansial harus mempertimbangkan biaya kepemilikan total (Total Cost of Ownership – TCO) yang bisa meliputi harga barang/jasa yang dibeli, biaya pelatihan karyawan, biaya perawatan (*maintenance cost*), biaya langganan (*subscription/license fee*), dan biaya-biaya yang terkait dengan pemerolehan barang/jasa yang dibeli.
g) Efisiensi finansial bisa mempertimbangkan antara keputusan membeli atau membuat sendiri sumber daya TIK. Selain itu juga bisa mempertimbangkan antara sewa/*outsourcing* dengan memiliki sumber daya TI baik dengan membuat sendiri maupun membeli.

Ketercapaian efisiensi dan efektivitas sumber daya informasi di setiap institusi pemerintah dicapai melalui:

1) Penyusunan arsitektur informasi yang mencerminkan kebutuhan informasi, struktur informasi dan pemetaan hak akses atas informasi oleh peran-peran yang ada dalam manajemen organisasi.

2) Identifikasi kebutuhan perangkat lunak aplikasi yang sesuai dengan spesifikasi arsitektur informasi, yang memungkinkan informasi diolah dan disampaikan kepada peran yang tepat secara efisien.

Efisiensi penggunaan teknologi (mencakup: platform aplikasi, software sistem, infrastruktur pemrosesan informasi, dan infrastruktur jaringan komunikasi) dicapai melalui konsep "mekanisme shared service" (baik di internal institusi pemerintahan atau antarinstitusi pemerintahan) yang meliputi:

i. Aplikasi, yaitu software aplikasi yang secara arsitektur teknis dapat dishare penggunaannya karena kesamaan kebutuhan fitur fungsionalitas. Perbedaan hanya sebatas di aspek konten informasi.
ii. Infrastruktur komunikasi: jaringan komputer/komunikasi, koneksi internet
iii. Data, yaitu keseluruhan data yang menjadi konten informasi. Pengelolaan data dilakukan dengan sistem Data Center/Disaster Recovery Center (DC/DRC)

G. Monitoring dan Evaluasi

Untuk memastikan adanya perbaikan berkesinambungan (continuous improvement), mekanisme monitoring & evaluasi akan memberikan umpan balik atas seluruh proses tata-kelola. Panduan umum monitoring dan evaluasi memberikan arahan tentang objek dan mekanisme monitoring dan evaluasi.

1. Objek Monitoring dan Evaluasi

   Ketercapaian indikator keberhasilan untuk setiap proses tata-kelola merupakan objek utama dari aktivitas monitoring & evaluasi. Indikator keberhasilan mencerminkan sejauh mana tujuan akhir dari setiap proses tata-kelola telah tercapai.

   Indikator kinerja proses dapat digunakan untuk melakukan penelusuran balik atas ketercapaian sebuah indikator keberhasilan. Variasi indikator kinerja proses diserahkan sepenuhnya kepada setiap instansi pemeritahan untuk menetapkannya sesuai dengan karakteristik proses manajemen yang dimilikinya.

2. Mekanisme Monitoring dan Evaluasi

   Pelaksanaan monitoring dan evaluasi harus mengakomodasi asas independensi, baik dilaksanakan secara internal maupun eksternal. Secara internal, setiap institusi pemerintahan melakukan evaluasi berupa peninjauan secara reguler atas ketercapaian indikator keberhasilan untuk setiap proses tata-kelola, di mana:

   a) Intensitas peninjauan indikator keberhasilan diserahkan kepada masing-masing institusi pemerintahan, setidaknya minimal 1 (satu) kali untuk setiap tahunnya.
   b) Setiap siklus peninjauan indikator keberhasilan harus didokumentasikan dan tindak lanjut atas rekomendasi dimonitor secara reguler oleh manajemen.
   c) Kerja sama dengan pihak ketiga dimungkinkan untuk pelaksanaan evaluasi secara internal, karena keterbatasan keahlian dan SDM, dengan spesifikasi kebutuhan detail tetap berasal dari institusi pemerintahan terkait.

Secara eksternal, dimungkinkan diadakannya evaluasi atas ketercapaian indikator keberhasilan sebuah institusi pemerintahan, di mana:

1) Inisiatif evaluasi eksternal berasal dari pihak di luar institusi pemerintahan yang akan menjadi objek evaluasi.
2) Tujuan utama evaluasi secara eksternal adalah mengetahui secara nasional atau cakupan wilayah tertentu ketercapaian tujuan tata-kelola TIK, dengan sudut pandang indikator keberhasilan yang relatif seragam.
3) Dewan TI Nasional berhak menetapkan pihak-pihak mana saja yang diberikan wewenang untuk melakukan evaluasi secara eksternal atas ketercapaian tujuan Tata-kelola TI di instansi-instansi pemerintahan.
4) Kerjasama dengan pihak ketiga dimungkinkan untuk pelaksanaan evaluasi secara eksternal, karena keterbatasan keahlian dan SDM, dengan spesifikasi kebutuhan detail tetap berasal dari institusi pemerintahan terkait.

[Halaman ini sengaja dikosongkan]

11

TEKNIK AUDIT DENGAN MICROSOFT EXCEL

A. Microsoft Excel

Microsoft Excel (Excel) adalah salah satu software yang dikeluarkan oleh Microsoft. Bentuk Excel terdiri dari sheet-sheet yang dikumpulkan dalam satu workbook. Excel dapat digunakan untuk menyelasaikan permasalahan administratif, mulai dari perhitungan sederhana sampai yang komplek dengan berbagai macam fungsi dan kebutuhan. Fungsi-fungsi yang dapat dijalankan oleh Excel antara lain:

1. Fungsi kalkulasi atau perhitungan dengan menggunakan data dari berbagai sel atau pehitungan sendiri.
2. Pembuatan grafik dengan berbagai macam jenis grafik.
3. Melakukan komunikasi dengan berbagai pengguna dalam jaringan komputer.
4. Pengiriman data dengan menggunakan internet.
5. Pehitungan dengan otomatisasi dari berbagai macam fungsi yang disediakan.
6. Perubahan atau modifikasi aplikasi dengan menggunakan fasilitas makro.

[Halaman ini sengaja dikosongkan]

12

PEMBAHASAN AUDIT PIUTANG

A. Deskripsi Piutang

Untuk mengetahui dengan jelas pengertian auditing, maka berikut ini akan dikemukakan definisi pengauditan yang diambil dari beberapa sumber:

1. Konrath (2002: 5) dalam Sukrisno Agoes (2004: 1) mendefinisikan audit sebagai

   "suatu proses sistematis untuk secara objektif mendapatkan dan mengevaluasi bukti mengenai asersi tentang kegiatan-kegiatan dan kejadian-kejadian ekonomi untuk meyakinkan tingkat keterkaitan antara asersi tersebut dan kriteria yang telah ditetapkan dan mengomunikasikan hasilnya kepada pihak-pihak yang berkepentingan."

2. Menurut Sukrisno Agoes (2004: 3), audit adalah

   "Suatu pemeriksaan yang dilakukan secara kritis dan sistematis oleh pihak yang independen, terhadap laporan keuangan yang telah disusun oleh manajemen beserta catatan-catatan pembukuan dan bukti-bukti pendukungnya, dengan tujuan untuk dapat memberikan pendapat mengenai kewajaran laporan keuangan tersebut.''

Piutang adalah tuntutan (*claims*) terhadap pihak tertentu yang penyelesaiannya diharapkan dalam bentuk Kas selama kegiatan normal perusahaan. Klaim timbul karena berbagai sebab. misalnya penjualan secara kredit, pemberian pinjaman kepada karyawan, persekot dalam kontrak pembelian, persekot kepada karyawan, dan lain-lain. Piutang usaha timbul karena adanya penyerahan barang atau jasa dalam rangka menjalankan kegiatan usaha normal perusahaan.

a) Jenis-jenis piutang
   1) Piutang dagang

      Piutang dagang terjadi akibat kegiatan normal suatu perusahaan melalui penjualan secara kredit, misalnya *notes receivable*.

   2) Piutang nondagang

      Merupakan piutang lainnya yang berasal bukan dari kegiatan utama perusahaan, misalnya penjualan surat berharga.

b) Sifat dan Contoh Piutang
   1) Sifat Piutang, menurut SAK:

      Digolongkan menurut sumber terjadinya

      1. Piutang Usaha → timbul dari penjualan barang dagangan atau jasa secara kredit

   2) Piutang Lain-lain → timbul dari transaksi di luar kegiatan usaha normal perusahaan

      i. Piutang Usaha dan Piutang Lain-lain yang diharapkan bisa ditagih dalam waktu satu tahun → Piutang Lancar

      ii. Piutang dinyatakan sebesar → jumlah tagihan dikurangi dengan taksiran jumlah yang tidak dapat ditagih

      iii. Jumlah kotor piutang harus tetap disajikan pada neraca, diikuti penyisihan untuk piutang yang tidak dapat ditagih

      iv. Perkiraan piutang pemegang saham dan piutang perusahaan afiliasi harus dilaporkan tersendiri (tidak digabung dengan perkiraan piutang), karena sifatnya yang berbeda.

   3) Contoh rekening yang digolongkan piutang :

      a. Piutang Usaha

      b. Wesel Tagih

c. Piutang Pegawai
d. Piutang Bunga
e. Uang Muka
f. *Refundable Deposit* (Uang Jaminan)
g. Piutang Lain-lain
h. *Allowance For Bad Debts* (Penyisihan Piutang Tak Tertagih)

B. Prinsip Akuntansi Piutang

Prinsip akuntansi piutang usaha:

1. Piutang usaha disajikan dalam neraca sebesar netto, yaitu piutang usaha dikurangi penyisihan kerugian piutang.
2. Metode penyisihan kerugian piutang usaha harus dijelaskan secukupnya.
3. Piutang usaha disajikan terpisah dengan piutang lain-lain.
4. Piutang yang bersaldo kredit disajikan sebagai kewajiban lancar dalam akun uang muka penjualan.
5. Piutang usaha yang dijadikan jaminan harus dijelaskan.

C. Tujuan Pemeriksaan *(Audit Objectives)* Piutang

1. Untuk memeriksa apakah terdapat *internal control* yang cukup baik atas piutang dan transaksi penjualan, piutang dan penerimaan kas, dengan ciri-ciri sebagai berikut:
   a) Adanya pemisahan tugas dan tanggung jawab yang melakukan penjualan, mengirimkan barang, melakukan penagihan, memberikan otorisasi atas penjualan kredit, membuat faktur penjualan dan melakukan pencatatan.
   b) Formulir yang digunakan bernomor urut tercetak *(prenumbered)*.
   c) Digunakan *price list* (daftar harga jual).
   d) Diadakannya sub buku besar piutang atau kartu piutang *(account receivable subledger card)*.
   e) Setiap akhir bulan: dibuat *aging schedule* piutang (analisis umur piutang), saldo piutang setiap pelanggan dibandingkan *(direconcile)* dengan saldo piutang menurut buku besar dan setiap pelanggan dikirim *monthly statement of account*.

f) Uang kas, check atau giro yang diterima dari pelanggan harus disetor dalam jumlah seutuhnya *(intact)*.

g) Mutasi kredit diperkiraan piutang (buku besar dan sub buku besar) yang berasal dari retur penjualan dan penghapusan harus diotorisasi oleh pejabat berwenang.

h) Setiap pinjaman yang diberikan kepada pegawai, direksi, pemegang saham dan perusahaan afiliasi harus diotorisasi oleh pejabat perusahaan yang berwenang.

i) Untuk memeriksa *validity* (keabsahan) dan *auhenticity* (ke ontetikan) piutang.

j) *Validity* → apakah piutang itu sah, masih berlaku (diakui oleh yang mempunyai utang).

k) *Authenticity* → apakah piutang itu didukung oleh bukti yang autentik yang ditandatangani pelanggan.

l) Untuk memeriksa *collectibility* dan cukup tidaknya perkiraan *allowance for bad debts*.

m) *Collectibility* → kemungkinan tertagihnya piutang (dalam neraca).

n) *Allowance for bad debts* → jumlah yang diperkirakan tidak bisa ditagih, harus dibuatkan penyisihan dalam jumlah yang cukup, jika sudah pasti tidak bisa ditagih harus dihapuskan.

o) *Allowance* terlalu besar → piutang disajikan terlalu kecil *(understated)*, biaya penyisihan piutang terlalu besar *(overstated)*, laba rugi *understated*.

p) *Allowance* terlalu kecil → piutang yang disajikan *overstated*, biaya penyisihan piutang *understated*, laba rugi *overstated*.

2. Untuk mengetahui apakah ada kewajiban bersyarat *(contingent liability)* yang timbul karena pendiskontoan wesel tagih *(notes receivable)*

   → Wesel tagih yang didiskontokan ke bank sebelum tanggal jatuh tempo, harus diungkapkan sebagai *contingent liability* pada tanggal neraca.

3. Untuk memeriksa apakah penyajian di neraca sesuai dengan prinsip akuntansi yang berlaku umum di Indonesia, sebagai berikut:

a) Piutang usaha, wesel tagih dan piutang lain-lain harus disajikan secara terpisah.
b) Piutang dinyatakan sebesar jumlah kotor tagihan dikurangi taksiran jumlah yang tidak dapat ditagih.
c) Saldo kredit piutang individual, jika jumlahnya material harus disajikan dalam kelompok kewajiban.

2. Dokumen atau Catatan yang Berkaitan
   a) Pesanan pelanggan (*customer order*).
   b) Pesanan penjualan (*sales order*).
   c) Faktur penjualan.
   d) File transaksi penjualan.
   e) Jurnal penjualan (*sales journal*).
   f) Credit note.
   g) Neraca saldo piutang usaha.
   h) Laporan bulanan.
   i) File induk piutang usaha.

[Halaman ini sengaja dikosongkan]

13

AUDIT SALDO PIUTANG USAHA

A. Piutang Usaha

Adalah piutang yang timbul dari transaksi penjualan barang atau jasa dalam kegiatan normal perusahaan. Piutang timbul apabila perusahaan menjual barang atau jasa kepada perusahaan lain atau perorangan secara kredit.

B. Prinsip Akuntansi Piutang Usaha

Piutang usaha disajikan di neraca sebesar jumlah yang diperkirakan dapat ditagih (pada tanggal neraca). Piutang usaha disajikan di neraca sebesar jumlah bruto dikurangi dengan taksiran/cadangan kerugian piutang tidak tertagih(CKP).

1) Jika tidak dibentuk cadangan kerugian piutang tidak tertagih, maka piutang disajikan dalam jumlah neto. Harus dicantumkan pengungkapan di neraca.
2) Jika piutang usaha bersaldo material, disajikan rinciannya di neraca.
3) Piutang usaha bersaldo kredit (di neraca), disajikan dalam kelompok utang lancar. Piutang nonusaha yang jumlahnya material, harus dipisahkan dari piutang usaha.

C. Asersi Manajemen Pada Piutang Usaha

1) Keberadaan atau keterjadian piutang usaha.
2) Kelengkapan piutang usaha.
3) Hak kepemilikan piutang usaha.
4) Penilaian piutang usaha.
5) Penyajian dan pengungkapan piutang usaha.

D. Tujuan Audit

1) Piutang usaha pada neraca saldo menurut umur cocok dengan jumlah pada file master dan jumlah total telah ditambahkan dengan tepat dan cocok dengan buku besar (Pengujian terinci).
2) Piutang usaha yang dicatat adalah ada (Keberadaan).
3) Piutang usaha yang ada telah dimasukkan semuanya (Kelengkapan).
4) Piutang usaha secara mekanis adalah akurat (Akurasi).
5) Piutang usaha diklasifikasikan dengan tepat (Klasifikasi).
6) Piutang usaha dicatat dalam periode(pisah batas) yang sesuai (Pisah batas).
7) Piutang usaha dinilai dengan memadai pada nilai yang dapat direalisir (Nilai yang direalisasi).
8) Piutang usaha benar-benar sah dimiliki klien (Hak).
9) Penyajian dan pengungkapan piutang usaha adalah memadai (Penyajian dan Pengukapan).

E. Program Pengujian Substantif Pada Piutang Usaha

Prosedur audit awal terhadap piutang usaha Mengusut saldo piutang usaha (dan CKP) yang tercantum di neraca, ke saldo akun piutang usaha di buku besar.

Menghitung kembali saldo akun piutang usaha di buku besar:

1) Saldo awal
2) Ditambah jumlah pendebitan,
3) Dikurangi jumlah pengkreditan me-*review* terhadap mutasi luar biasa pada akun piutang usaha dan akun cadangan kerugian piutang (CKP).

Mengusut saldo awal akun piutang usaha dan CKP (di buku besar) ke kertas kerja tahun yang lalu. Mengusut posting pendebitan dan pengkreditan akun piutang usaha (dan akun CKP) ke jurnal. Merekonsiliasi akun piutang usaha (di buku besar) ke buku pembantu piutang usaha.

Prosedur analitik atas piutang usaha Perhitungan rasio-rasio keuangan yang berkaitan dengan piutang usaha. Rasio-rasio membantu auditor dalam mengungkapkan:

1) Peristiwa atau transaksi yang tidak biasa
2) Perubahan akuntansi
3) Perubahan usaha
4) Fluktuasi acak
5) Salah saji

F. Rasio-rasio pada Piutang Usaha

1) Rasio tingkat perputaran piutang usaha.
2) Rasio piutang usaha dengan aktiva lancar.
3) Rasio rate *of return on sales*.
4) Rasio kerugian piutang usaha dengan penjualan bersih.
5) Rasio kerugian piutang usaha dengan piutang usaha yang sesungguhnya tidak tertagih.

G. Pengujian Terinci Atas Saldo

Pengujian terinci atas saldo-saldo untuk semua siklus langsung diarahkan pada akun-akun neraca, akun laporan laba rugi tidak diabaikan tetapi akan diverifikasi sebagai hasil sampingan dengan pengujian neraca. Konfirmasi piutang usaha merupakan pengujian terinci atas piutang usaha yang paling penting.

H. Konfirmasi Pada Piutang Usaha

Tujuan utama konfirmasi piutang usaha adalah untuk memenuhi tujuan keabsahan penilaian, dan pisah batas. Persyaratan AICPA Ada dua prosedur audit yang diwajibkan oleh AICPA mengenai bahan bukti: konfirmasi piutang usaha dan pemeriksaan fisik persediaan. Persyaratan

untuk konfirmasi dimodifikasi agar laporan wajar tanpa pengecualian dapat diterbitkan sekalipun piutang usaha tidak dikonfirmasi asalkan salah satu dari tiga kondisi berikut terpenuhi:

1) piutang usaha tidak material,
2) pertimbangan auditor akan ketidakefektifan konfirmasi karena tingkat respons tidak cukup dan tidak andal,
3) gabungan tingkat risiko bawaan dan risiko pengendalian sedemikian rendah dan bahan bukti yang substantif lain dapat dikumpulkan untuk memberikan bahan bukti yang cukup.

I. Jenis Konfirmasi yang Lazim Digunakan

1) Konfirmasi positif, konfirmasi secara langsung kepada debitur apakah saldo yang dinyatakan benar atau tidak, atau meminta debitur menuliskan saldo atau melengkapi informasi lain(form konfirmasi kosong). Lebih andal tapi agak mahal.
2) Konfirmasi negatif, hanya meminta jawaban kalau debitur tidak sepakat dengan jumlah yang dinyatakan. Lebih murah tapi kurang andal. Konfirmasi negatif dapat diterima hanya jika semua kondisi berikut terpenuhi: bersaldo akun kecil; gabungan risiko pengendalian yang ditetapkan dan risiko bawaan adalah rendah.

Saat pelaksanaan konfirmasi agar diperoleh bahan bukti yang andal bila dikirimkan sedekat mungkin dengan tanggal neraca, yang memungkinkan auditor menguji secara langsung saldo piutang pada laporan keuangan tanpa perlu memperhitungkan transaksi yang terjadi di antara tanggal konfirmasi dan tanggal neraca. Faktor lain yang mempengaruhi adalah materialitas piutang usaha dan risiko perkara hukum bagi auditor karena kemungkinan bangkrutnya klien dan risiko sejenis. Ukuran sampel konfirmasi dipengaruhi oleh beberapa faktor: salah saji yang ditolelir, risiko bawaan, risiko pengendalian, risiko deteksi yang dicapai dengan pengujian substantif lain, dan jenis konfirmasi.

J. Surat Representasi mengenai Piutang Usaha

Surat representasi mengenai piutang usaha merupakan pernyataan dari klien bahwa tanggung jawab atas kewajaran informasi yang disajikan dalam laporan keuangan berada di tangan klien, bukan pada auditor.

Isi surat representasi mengenai piutang usaha adalah:

1) Klaim yang sah atas piutang usaha.
2) Piutang tidak dijadikan jaminan utang.
3) Barang yang dikonsinyasi telah dipisahkan dari piutang.
4) Piutang yang tidak dapat ditagih telah dihapus.
5) CKP cukup untuk menutup kerugian piutang tidak tertagih yang diperkirakan.

[Halaman ini sengaja dikosongkan]

14

AUDIT SIKLUS PIUTANG PADA PERUSAHAAN DAGANG

A. Tujuan Audit

Tujuan audit ini adalah: untuk mengevaluasi apakah saldo-saldo yang dipengaruhi oleh siklus ini telah disajikan secara wajar sesuai dengan standar akuntansi yang berlaku umum.

Fungsi bisnis pada siklus penjualan dan penerimaan kas terdiri dari:

1. Pemrosesan Pesanan Pelanggan

   Merupakan awal dari siklus dan berupa penawaran untuk membeli barang dengan ketentuan tertentu. Dokumen yang berhubungan: Pesanan pelanggan (*customer order*), Pesanan penjualan (*sales order*).

2. Persetujuan Penjualan Kredit

   Praktik yang lemah menyebabkan piutang tak tertagih besar. Persetujuan penjualan kredit ditandai oleh persetujuan untuk mengirim barang.

3. Pengiriman Barang

   Nota pengiriman disiapkan saat penjualan dan dokumen pengiriman (*bill of landing*) dibuat untuk keperluan penagihan atas pengiriman ke pelanggan. Dokumen yang berhubungan:

a) Dokumen pengiriman (*shipping document*)
b) Faktur penjualan (*sales invoice*)
c) Jurnal penjualan (*sales journal*)
d) Neraca saldo A/R
e) Laporan ikhtisar penjualan (*summary sale report*)
f) Laporan Bulanan (*Monthly Statement*)
g) Berkas induk piutang dagang (A/R *Master file*).

4. Proses dan Pencatatan Penerimaan Kas

   Meliputi penerimaan, penyimpanan, dan pencatatan kas baik kas maupun berupa cek. Pertimbangan utama adalah seluruh kas harus disetor ke bank dalam jumlah yang benar dengan tepat waktu dan dicatat ke berkas transaksi penerimaan kas yang digunakan untuk membuat jurnal penerimaan kas dan memutakhirkan berkas induk piutang usaha.

   Dokumen yang berhubungan:

   a) Nota pembayaran (*Remittance Advice*)
   b) Daftar awal penerimaan kas
   c) Jurnal penerimaan kas.

B. Memperkirakan Risiko Pengendalian yang Direncanakan Penjualan

Dengan empat langkah dasar:

1. Auditor membutuhkan kerangka dasar untuk memperkirakan risiko pengendalian.
2. Auditor harus mengidentifikasi pengendalian intern kunci dan kelemahan atas transaksi pengendalian.
3. Auditor menghubungkan pengendalian dan kelemahan dengan tujuan.
4. Auditor memperkirakan risiko pengendalian pada setiap tujuan dengan mengevaluasi pengendalian dan kelemahan untuk setiap tujuan.

Pengendalian kunci terdiri dari:

a) Pemisahan tugas yang memadai.
b) Otorisasi yang semestinya.
c) Dokumen/catatan yang memadai.
d) Dokumen yang prenumbered.
e) Pengiriman *monthly statement*.
f) Prosedur verifikasi intern.

5. Mengevaluasi Untung Rugi Pengujian atas Pengendalian.
6. Merancang Pengujian atas Pengendalian untuk Transaksi Penjualan.
7. Merancang Pengujian Substantif atas Transaksi Penjualan.

   Bertujuan untuk:

   a) Penjualan yang dicatat benar-benar ada.

      Terdapat dua kemungkinan salah saji: penjualan dicatat untuk pengiriman yang tidak pernah dilakukan dan pengiriman dilakukan ke pelanggan fiktif dan dicatat sebagai penjualan.

      Sifat pengujian tergantung sifat kelemahan Internal Control; dengan menelusuri dari jurnal ke dokumen dasar (*test of ommission*)

   b) Transaksi penjualan yang terjadi telah dicatat

      Dengan menelusuri dari dokumen dasar ke jurnal di mana dokumen sebagai *direction of test*.

   c) Penjualan dicatat secara akurat

      Kebenaran penilaian transaksi penjualan berkenaan dengan pengiriman jumlah barang yang dipesan, kebenaran penagihan atas jumlah yang dikirim dan kebenaran pencatatan jumlah yang ditagih dalam catatan akuntansi.

   d) Penjualan yang dicatat telah diklasifikasikan sebagaimana mestinya

      Pengujian atas klasifikasi penjualan merupakan bagian pengujian penilaian.

   e) Penjualan dicatat pada tanggal yang tepat

      Penjualan ditagih dan dicatat sesegera mungkin setelah terjadinya pengiriman untuk mencegah hilangnya transaksi

dari catatan tanpa sengaja dan untuk menjamin bahwa penjualan dicatat pada periode yang sesuai.

f) Transaksi penjualan dicatat dengan semestinya di berkas induk dan diikhtisarkan dengan benar.

Dalam siklus kegiatan perusahaan atau dalam jangka waktu satu tahun klaim atas barang atau jasa, serta uang kepada pihak lain disebut dengan piutang. Di neraca, penyajian piutang dibagi menjadi 2 kelompok yaitu piutang nonusaha dan piutang usaha. Transaksi penjualan dapat menjadi penyebab dari timbulnya piutang usaha. Sedangkan, penyebab timbulnya piutang usaha adalah transaksi yang tidak berkaitan dengan transaksi penjualan. Contoh dari piutang nonusaha adalah piutang pengenbalian pajak, piutang dividen dan bunga, piutang penjualan saham, dan piutang kepada karyawan. Dari segi material, piutang usaha lebih besar jumlah materialnya daripada piutang nonusaha.

Di Neraca Piutang Usaha Disajikan Berdasarkan Prinsip Akuntansi Berterima Umum

1. Di neraca penyajian piutang usaha harus didasarkan pada perkiraan berapa jumlah yang akan diberikan oleh kreditur di tanggal neraca tersebut. Di neraca penyajian piutang usaha adalah jumlah bruto dikurangi dengan taksiran kerugian piutang tak tertagih.
2. Pembentukan cadangan kerugian piutang harus dicantumkan di neraca.
3. Di neraca harus disajikan rincian saldo piutang yang material.
4. Kelompok utang lancar juga berisi adanya piutang dengan saldo kredit pada tanggal neraca.
5. Piutang usaha yang jumlahnya material disajikan secara terpisah dari piutang usaha.

Berikut Adalah Tujuan Pengendalian Piutang Usaha.

1. Membuktikan keandalan catatan akuntansi tentang piutang usaha untuk memperoleh keyakinan.
2. Sebagai pembuktian Piutang usaha yang disajikan di neraca tentang kebenarannya dan keterjadian transaksinya.
3. Sebagai pembuktian kelengkapan mengenai saldo piutang usaha di neraca serta catatan akuntansi.

4. Sebagai pembuktian hak kepemilikan piutang usaha yang disajikan di neraca.
5. Sebagai pembuktian mengenai kewajaran dalam penilaian piutang usaha yang disajikan dalam neraca.
6. Sebagai pembuktian atas kewajaran dalam pengungkapan dan penyajian piutang usaha dalam neraca.

Audit Terhadap Piutang Usaha

Prosedur audit awal

1. Lakukan prosedur berikut ini.
   a) Saldo yang ada di neraca diusut ke saldo piutang usaha si buku besar.
   b) Saldo piutang usaha di buku besar dihitung kembali.
   c) Adakan *review* mutasi luar biasa baik sumber posting maupun jumlah di akun Cadangan Kerugian Piutang Usaha dan akun Piutang Usaha.
   d) Saldo awal pada akun Cadangan Kerugian Piutang serta akun Piutang Usaha diusut ke kertas kerja tahun lalu.
   e) akun Piutang Usaha dengan posting debit diusut ke jurnal yang terkait.
   f) Adakan rekonsiliasi buku besar ke buku pembantu utang usaha mengenai akun kontrol piutang usaha.

Prosedur Analitik

2. Lakukan prosedur analitik
   a) Pertama lakukan perhitungan ratio atas data berikut.
      - Tingkat perputaran terhadap piutang
      - Ratio antara aktiva lancar dengan piutang usaha
      - *Rate of return on sales*
      - Rasio antara penjualan kredit dengan kerugian piutang usaha
      - Rasio antara jumlah riil piutang usaha yang tak tertagih dengan kerugian piutang usaha.
   b) Adakan analisis antara data yang didasarkan pada tahun lalu, jumlah yang dianggarkan, data industri melalui prosedur analitik.

Pengujian terhadap Transaksi Rinci

3. Lakukan periksaan atas sampel transaksi piutang yang telah dicatat ke dokumen yang terkait dengan piutang usaha.
   a. Lakukan pemeriksaan akun piutang usaha yang dilakukan pendebitan ke dokumen pendukung piutang seperti laporan pengiriman barang, order penjualan, dan faktur penjualan.
   b. Lakukan pemeriksaan akun piutang usaha yang dilakukan pengkreditan ke dokumen pendukung piutang seperti penghapusan piutang atau rabat penjualan, retur atau memo kredit, serta bukti kas masuk.
4. Lakukan verifikasi terhadap pisah batas antara retur penjualan dan transaksi penjualan
   a. Lakukan pemeriksaan terhadap dokumen pendukung piutang minggu pertama setelah tanggal neraca maupun minggu terakhir tahun yang diaudit.
   b. Lakukan pemeriksaan atas dokumen pendukung berkurangnya piutang usaha baik minggu pertama setelah tanggal neraca maupun minggu terakhir tahun yang diaudit.
5. Lakukan verifikasi pisah batas atas transaksi penerimaan kas.
   a. Lakukan observasi untuk melihat semua kas yang diterima pada hari terakhir tahun yang diaudit terhadap setoran perjalanan dan penerimaan kas tahun berikutnya sebagai penerimaan kas di tahun yang sedang diaudit.
   b. Lakukan *review* atas dokumen berikut yaitu salinan bukti setor, rekening koran, ringkasan transaksi kas secara harian untuk beberapa hari sebelum maupun sesudahnya.

Pengujian terhadap saldo akun rinci

6. Lakukan sebuah konfirmasi atas piutang.
   a. Tentukanlah metode, waktu, dan serta seberapa luas konfirmasi yang akan dilaksanakan.
   b. Pilihlah debitur untuk dikirimi surat konfirmasi dan kemudian lakukan pengiriman konfirmasi.
   c. Konfirmasi yang positif yang tidak memperoleh jawaban, maka prosedur alternatif berikut perlu dilaksanakan.

- Lakukan pemeriksaan dokumen pendukung atas pencatatan penerimaan kas yang diperoleh dari debitur setelah tanggal neraca.
- Lakukan pemeriksaan dokumen pendukung atas akun piutang baik berupa pengkreditan dan pendebitan kepada debitur.

7. Lakukan sebuah evaluasi atas akun Cadangan Kerugian Piutang dari klien
   a. Lakukan cocokkan akun piutang usaha dalam buku besar dengan jumlah saldo piutang serta lakukan footing dan cross-footing daftar saldo piutang.
   b. Lakukan sebuah pengujian atas penentuan umur piutang usaha dari klien.
   c. Lakukan perbandingan cadangan cadangan kerugian piutang usaha yang tercantum dalam neraca tahun sebelumnya dengan neraca tahun yang diaudit.
   d. Lakukan pemeriksaan yang utangnya telah lewat waktu atau kedaluwarsa dengan catatan kredit untuk debitur.

   Verifikasi pengungkapan dan penyajian

8. Lakukan perbandingan atas piutang usaha antara prinsip akuntansi berterima umum dengan neraca
   a. Lakukan pemeriksaan klasifikasi atas piutang usaha dalam aktiva tidak lancar maupun kelompok aktiva lancar.
   b. Lakukan pemeriksaan jawaban dari konfirmasi bank.
   c. Lakukan pemeriksaan klasifikasi atas piutang ke kelompok piutang non-usaha dan piutang usaha.
   d. Lakukan pemeriksaan akuntansi untuk piutang serta pengungkapannya mengenai anjak piutang, piutang yang digadaikan, serta antarpihak yang memiliki hubungan istimewa.
   e. Periksa surat representasi klien mengenai piutang, sesudah tanggal neraca, untuk menentukan ketepatan pisah batas.

[Halaman ini sengaja dikosongkan]

DAFTAR PUSTAKA

Alvin A, Arens, James K.Loebbecke, (2003). *Auditing*, Edisi Indonesia, Jakarta: Erlangga.

Anonim. 2010. Standar dan metode auditing pada sistem PDE. (online) (http://zetzu.blogspot.com/2010/10/standar-dan-metode-auditing-pada-sistem.html. Diakses pada tanggal 25 November 2014).

Information System Audit and Control Association (ISACA) (2003), *IS Standards, Guidelines and Procedures for Auditing and Control Professionals*, diakses 14 Juli 2003.

IT Governance Institute (2000), *Executive Summary*, COBIT 3rd Edition, http://www.isaca.org, diakses 14 Juli 2003.

IT Governance Institute (2000), *Audit Guidelines*, COBIT 3rd Edition, http://www.isaca.org, diakses 14 Juli 2003.

IT Governance Institute (2000), *Management Guidelines*, COBIT 3rd Edition, http://www.isaca.org., diakses 14 Juli 2003.

IT Governance Institute (2000), *Implemetation Tool Set*, COBIT 3rd Edition, http://www.isaca.org., diakses 14 Juli 2003.

Masguh. 2010. Perbedaan audit pde dan audit konvensional. (online) (http://kuliahhurahura.blogspot.com/2010/04/perbedaan-audit-pde-dan-audit.html. Diakses pada tanggal 25 November 2014)

Qiqie. 2011. *Mengaudit Pusat PDE dan Aplikasi Komputer.* (online) (http://qiqie-novrianty.blogspot.com/2011_03_01_archive.html. Diakses pada tanggal 26 November 2014).

Syahroni, Ahmad. 2013. *Pengertian Data Elektronik*. (online) (http://ahmadsyahroni-jepara.blogspot.com/2013/01/pengertian-pengolahan-data-elektronik.html. Diakses pada tanggal 25 November 2014).

Weber, Ron (1999), *Information Systems Control and Audit*, Prentice Hall: The University of Queensland.

Yayasan Pendidikan Internal Audit (2002), *Institut Pendidikan dan Pelatihan Audit dan Manajemen*, Audit Sistem Informasi II, Jakarta.

BIODATA PENULIS

Aloysius Harry Mukti, M.S.Ak., Ph.D., Penulis menyelesaikan S1 pada Progam Studi Akuntansi di Universitas Widyatama, Menempuh pendidikan S2 pada Program Pascasarjana Ilmu Akuntansi Universitas Indonesia dan memperoleh gelar Doktor Ilmu Manajemen dari Philippine Christian University, Manila, Philippines. Saat ini Penulis juga sedang menyelesaikan studi S1 di Fakultas Hukum Universitas Trisakti.

Selain aktif sebagai Komite Audit juga merupakan pengajar pada Universitas Bhayangkara Jakarta Raya dan beberapa Institusi atau Perguruan tinggi lain seperti Politeknik Keuangan Negara STAN, Universitas Pelita Harapan dan Institut Bisnis Nusantara.

Dr. Istianingsih Sastrodihardjo. M.S.Ak, CA., CSRS., CSRA., CMA., CBV., CACP. Penulis menyelesaikan S1 pada Program Studi Manajemen di Universitas Terbuka dan S1 Program Studi Akuntansi di Universitas Mercu Buana Jakarta. Mengambil Program A4 di Universitas Negeri Jakarta dan Program Pendidikan Profesi Akuntansi Universitas Trisakti. Menempuh pendidikan S2 pada Program Pascasarjana Ilmu Akuntansi Universitas Indonesia, dan memperoleh gelar Doktor Ilmu Akuntansi dengan predikat Yudisium Cumlaude pertama dari Program Doktor Ilmu Akuntansi Universitas Indonesia. Penulis juga sudah selesai menjalani Program PostDoctoral di Murdoch University, Perth, Australia.

Founder Karisma-Consulting dan Direktur utama PT. Karisma Metadata Sinergi ini merupakan Ketua Forum Dosen Akuntansi Perguruan Tinggi DKI-Ikatan Akuntansi Indonesia. Selain mengajar pada Program Studi Magister di Institut Bisnis Nusantara dan STEI Jakarta serta program Doktor Akuntansi Universitas Trisakti, saat ini penulis juga menjabat sebagai Dekan Fakultas Ekonomi dan Bisnis Universitas Bhayangkara Jakarta Raya.

REPUBLIK INDONESIA
KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA

SURAT PENCATATAN
CIPTAAN

Dalam rangka pelindungan ciptaan di bidang ilmu pengetahuan, seni dan sastra berdasarkan Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta, dengan ini menerangkan:

Nomor dan tanggal permohonan	:	EC00202376922, 5 September 2023
Pencipta		
Nama	:	**Aloysius Harry Mukti, M.S.Ak., Ph.D dan Dr. Istianingsih, M.S.Ak, CA, CSRS, CSRA, CMA, CBV, CACP**
Alamat	:	Bintaro Park View RT 03/ RW 03, Pesanggrahan, Kota Jakarta Selatan, Pesanggrahan, Jakarta Selatan, DKI Jakarta, 12320
Kewarganegaraan	:	Indonesia
Pemegang Hak Cipta		
Nama	:	**Aloysius Harry Mukti, M.S.Ak., Ph.D, Dr. Istianingsih, M.S.Ak, CA, CSRS, CSRA, CMA, CBV, CACP dkk**
Alamat	:	Bintaro Park View RT 03/ RW 03, Pesanggrahan, Kota Jakarta Selatan, Pesanggrahan, Jakarta Selatan, DKI Jakarta, 12320
Kewarganegaraan	:	Indonesia
Jenis Ciptaan	:	**Buku**
Judul Ciptaan	:	**Audit Pengolahan Data Elektronik**
Tanggal dan tempat diumumkan untuk pertama kali di wilayah Indonesia atau di luar wilayah Indonesia	:	30 September 2021, di Depok
Jangka waktu pelindungan	:	Berlaku selama 50 (lima puluh) tahun sejak Ciptaan tersebut pertama kali dilakukan Pengumuman.
Nomor pencatatan	:	000509875

adalah benar berdasarkan keterangan yang diberikan oleh Pemohon.
Surat Pencatatan Hak Cipta atau produk Hak terkait ini sesuai dengan Pasal 72 Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta.

a.n. MENTERI HUKUM DAN HAK ASASI MANUSIA
Direktur Hak Cipta dan Desain Industri

Anggoro Dasananto
NIP. 196412081991031002

Disclaimer:
Dalam hal pemohon memberikan keterangan tidak sesuai dengan surat pernyataan, Menteri berwenang untuk mencabut surat pencatatan permohonan.

LAMPIRAN PEMEGANG

No	Nama	Alamat
1	Aloysius Harry Mukti, M.S.Ak., Ph.D	Bintaro Park View RT 03/ RW 03, Pesanggrahan, Kota Jakarta Selatan
2	Dr. Istianingsih, M.S.Ak, CA, CSRS, CSRA, CMA, CBV, CACP	Jl. Perjuangan No 81, RT 003/ RW 002, Marga Mulya, Kec. Bekasi Utara
3	Lembaga Penelitian, Pengabdian Kepada Masyarakat dan Publikasi (LPPMP) Universitas Bhayangkara Jakarta Raya	Jl. Perjuangan No 81, RT 003/ RW 002, Marga Mulya, Kec. Bekasi Utara