untuk proses control (pengendalian) ada tindakan yang perlu dilaksanakan, gunaka referensi yang ada untuk menjawap pertanyaan saya tertutama dalam hal pengembangan sistem, pemrogramaan dan operasional

PENGEMBANGAN SISTEM DAN PROGRAM PENGGANTIAN KEGIATAN

Kemudian menguraikan kegiatan utama yang merupakan siklus hidup pengembangan sistem (SDLC). Ini termasuk perencanaan sistem, analisis sistem, desain konseptual, sistem seleksi, desain rinci, implementasi sistem, dan prosedur perubahan Program (sistem pemeliharaan).

A. PESERTA DALAM PEMBANGUNAN SISTEM

1. Sistem profesional ada sistem analis, insinyur sistem, dan programmer.
2. Pengguna akhir adalah mereka yang sistem dibangun.
3. Stakeholder
4. Akuntan / Auditor

Mengapa Akuntan dan Auditor Terlibat dengan SDLC?

1) Penciptaan sistem informasi memerlukan transaksi keuangan yang signifikan.
2) Perhatian kedua dan yang lebih mendesak untuk akuntan dan auditor adalah dengan sifat produk yang muncul dari SDLC.

Bagaimana Apakah Akuntan Terlibat dengan SDLC?

a. Akuntan adalah pengguna.
b. Akuntan berpartisipasi dalam pengembangan sistem sebagai anggota tim pengembangan.
c. Akuntan terlibat dalam pengembangan sistem sebagai auditor. Sistem informasi akuntansi harus dapat diaudit.

B. SISTEM INFORMASI AKUISISI

1. Pengembangan In-House
2. Sistem Komersial
    a. Sebuah Tren Software Komersial
        1) Biaya yang relatif rendah perangkat lunak komersial umum dibandingkan dengan perangkat lunak yang disesuaikan;
        2) Munculnya vendor industri-spesifik yang menargetkan perangkat lunak mereka dengan kebutuhan jenis tertentu dari bisnis;
        3) Sebuah permintaan dari bisnis yang terlalu kecil untuk mampu staf pengembangan sistem 'di-rumah; dan
        4) Kecenderungan menuju perampingan dari unit organisasi dan gerakan yang dihasilkan terhadap lingkungan pengolahan data terdistribusi, yang telah membuat pilihan perangkat lunak komersial lebih menarik bagi organisasi yang lebih besar.

b. Jenis Sistem Komersial

1) Turnkey Sistem
2) Sistem Akuntansi Umum
3) Sistem tujuan khusus
4) Sistem Otomasi Kantor.
5) Sistem Backbone.
6) Penjual-Didukung Sistem

Keuntungan Software Komersial

- Waktu Pelaksanaan
- Biaya
- Keandalan

Kekurangan Software Komersial

- Kemerdekaan
- Kebutuhan untuk kustomisasi sistem
- Pemeliharaan

C. SISTEM PEMBANGUNAN SIKLUS HIDUP

1. Sistem Perencanaan - Tahap 1

a. Siapa yang Harus Dilakukan Perencanaan Sistem? Tanggung jawab khas untuk komite pengarah meliputi berikut ini:
   1) Menyelesaikan konflik yang timbul dari sistem baru
   2) Meninjau proyek dan menetapkan prioritas
   3) dana Anggaran untuk pengembangan sistem
   4) Mengkaji status proyek individu dalam pengembangan
   5) Menentukan di berbagai pos pemeriksaan di seluruh SDLC apakah akan melanjutkan dengan proyek atau mengakhiri itu

b. Perencanaan Strategis Sistem

   Perencanaan sistem strategis melibatkan alokasi sumber daya sistem di tingkat makro. Biasanya berkaitan dengan kerangka waktu 3 sampai 5 tahun. Proses ini mirip dengan sumber anggaran untuk kegiatan strategis lainnya, seperti pengembangan produk, perluasan tanaman, riset pasar, dan teknologi manufaktur.

   Secara teknis, perencanaan sistem strategis bukan bagian dari SDLC karena SDLC berkaitan dengan aplikasi tertentu. Sistem strategis rencana berkaitan dengan alokasi sumber daya seperti sistem sebagai karyawan (jumlah sistem profesional untuk dipekerjakan), hardware (jumlah workstation, minicomputer, dan mainframe yang

akan dibeli), perangkat lunak (dana yang akan dialokasikan untuk proyek-proyek baru dan sistem untuk sistem pemeliharaan), dan telekomunikasi (dana yang dialokasikan untuk jaringan dan EDI). Adalah penting bahwa rencana strategis menghindari detail yang berlebihan. Rencana harus memungkinkan spesialis sistem untuk membuat keputusan dengan mempertimbangkan faktor-faktor yang relevan seperti harga, ukuran kinerja, ukuran, keamanan, dan kontrol.

Mengapa Melakukan Perencanaan Strategis Sistem? Ada empat pembenaran untuk perencanaan sistem strategis:

1) Sebuah rencana yang berubah secara konstan lebih baik daripada tidak ada rencana sama sekali.
2) Perencanaan strategis mengurangi komponen krisis dalam pengembangan sistem.
3) Perencanaan sistem Strategis menyediakan kontrol otorisasi untuk SDLC.
4) Biaya manajemen.

c. Perencanaan proyek
   1) Tujuan dari perencanaan proyek adalah untuk mengalokasikan sumber daya untuk aplikasi individual dalam kerangka rencana strategis.
   2) Usulan proyek menyediakan manajemen dengan dasar untuk memutuskan apakah akan melanjutkan proyek tersebut.
      a) Merangkum temuan dari studi yang dilakukan ke titik ini menjadi rekomendasi umum untuk sistem baru atau diubah.
      b) Proposal menguraikan keterkaitan antara tujuan dari sistem yang diusulkan dan tujuan bisnis perusahaan, terutama yang digariskan dalam rencana strategis IT
      c) Jadwal proyek merupakan komitmen manajemen untuk proyek.

d. Peran Auditor dalam Perencanaan Sistem

   Auditor secara rutin memeriksa tahap perencanaan sistem SDLC. Perencanaan sangat mengurangi risiko bahwa suatu organisasi telah menghasilkan tidak dibutuhkan, tidak efisien, tidak efektif, dan penipuan sistem. Oleh karena itu, auditor internal dan eksternal tertarik dalam memastikan bahwa perencanaan sistem yang memadai berlangsung.

2. Analisis Sistem - Tahap 2

a. Langkah Survei
   1) Kekurangan Survei Sistem sekarang
      a) Current physical pit tar
      b) Berpikir di dalam kotak.

2) Keuntungan dari Survei Sistem sekarang
    a) Mengidentifikasi aspek apa dari sistem lama harus disimpan.
    b) Memaksa Sistem analis untuk memahami sistem.
    c) Mengisolasi akar gejala masalah

b. Pengumpulan Fakta
    1) Sumber data
    2) Pengguna
    3) Proses
    4) Aliran data
    5) Kontrol
    6) Volume transaksi
    7) Tingkat Kesalahan
    8) Biaya Sumber Daya
    9) Hambatan dan operasi berlebihan

c. Teknik fakta-Temu
    1) Observasi
    2) Partisipasi Tugas
    3) Wawancara Pribadi
        a) Buka-berakhir pertanyaan
        b) Quessionaires
    4) Meninjau Dokumen Key

    Dokumen organisasi adalah sumber lain dari fakta tentang sistem yang disurvei. Contoh ini meliputi berikut ini:

    a) grafik Organisasi
    b) Deskripsi pekerjaan
    c) catatan Akuntansi
    d) Grafik rekening
    e) pernyataan Kebijakan
    f) Deskripsi prosedur
    g) Laporan keuangan
    h) Laporan Kinerja
    i) flowchart Sistem
    j) Dokumen sumber
    k) listing Transaksi
    l) Anggaran
    m) Prakiraan
    n) pernyataan Misi

d. Analisis Langkah

Analisis sistem adalah proses intelektual yang bercampur dengan pengumpulan fakta. Analis secara bersamaan menganalisis karena ia mengumpulkan fakta-fakta. Pengakuan belaka masalah mengandaikan beberapa pemahaman tentang norma atau keadaan yang diinginkan. Oleh karena itu sulit untuk mengidentifikasi di mana survei berakhir dan analisis dimulai.

e. Analisis sistem Laporan

Acara yang menandai kesimpulan dari tahap analisis sistem adalah penyusunan sistem analisis laporan resmi. Laporan ini menyajikan kepada manajemen atau komite pengarah temuan survei, masalah yang diidentifikasi dengan sistem saat ini, kebutuhan pengguna, dan persyaratan sistem baru. Gambar 5.3 berisi format yang mungkin untuk laporan ini. Tujuan utama untuk melakukan analisis sistem adalah untuk mengidentifikasi kebutuhan pengguna dan menentukan persyaratan untuk sistem baru. Laporan tersebut harus diatur secara rinci apa sistem harus lakukan, bukan bagaimana melakukannya. Pernyataan persyaratan dalam laporan menetapkan pemahaman antara sistem profesional, manajemen, pengguna, dan pemangku kepentingan lainnya. Dokumen ini merupakan kontrak resmi yang menentukan tujuan dan sasaran dari sistem. Sistem analisis laporan harus membentuk segi jelas sumber data, pengguna, file data, proses umum, arus data, kontrol, dan kapasitas volume transaksi.

Laporan analisis sistem tidak menentukan desain rinci dari sistem yang diusulkan. Sebagai contoh, tidak menentukan metode pengolahan, media penyimpanan, struktur record, dan rincian lain yang diperlukan untuk merancang sistem fisik. Sebaliknya, laporan tersebut tetap pada tingkat tujuan untuk menghindari menempatkan kendala buatan pada tahap desain konseptual. Beberapa desain yang mungkin dapat melayani kebutuhan pengguna, dan proses pembangunan harus bebas untuk mengeksplorasi semua ini.

f. Peran Auditor dalam Analisis Sistem

Auditor perusahaan (baik eksternal dan internal) merupakan pemangku kepentingan dalam sistem yang diusulkan. Dalam Bab 8, kita akan melihat bagaimana tertentu CAATTs (seperti modul audit tertanam dan fasilitas uji terintegrasi) harus dirancang ke dalam sistem selama SDLC. Seringkali, fitur pemeriksaan lanjutan tidak dapat dengan mudah ditambahkan ke sistem yang ada. Oleh karena itu, akuntan / auditor harus terlibat dalam analisis kebutuhan sistem yang diusulkan untuk menentukan apakah itu adalah calon yang baik untuk fitur audit yang canggih dan, jika demikian, yang fitur yang paling cocok untuk sistem.

3. Sistem Konseptual Desain - Tahap 3

Tujuan dari tahap desain konseptual adalah untuk menghasilkan beberapa sistem konseptual alternatif yang memenuhi persyaratan sistem yang diidentifikasi selama analisis sistem.

a. Desain Pendekatan Terstruktur

Pendekatan desain terstruktur adalah cara disiplin merancang sistem dari atas ke bawah. Ini terdiri dari dimulai dengan "gambaran besar" dari sistem yang diusulkan yang secara bertahap didekomposisi menjadi lebih dan lebih rinci sampai dipahami sepenuhnya. Dalam pendekatan ini, proses bisnis di bawah desain biasanya didokumentasikan oleh aliran data dan diagram struktur. Gambar 5.4 menunjukkan penggunaan diagram aliran data (DFD) dan diagram struktur untuk menggambarkan dekomposisi top-down dari proses bisnis hipotetis.

Tahap desain konseptual harus menyoroti perbedaan antara fitur penting dari sistem bersaing daripada kesamaan mereka. Oleh karena itu, desain sistem pada saat ini harus umum. Desain harus mengidentifikasi semua input, output, proses, dan fitur-fitur khusus yang diperlukan untuk membedakan satu alternatif dari yang lain. Gambar 5.5 menyajikan dua desain konseptual alternatif untuk sistem pembelian. Desain ini tidak memiliki rincian yang diperlukan untuk mengimplementasikan sistem. Misalnya, mereka tidak termasuk komponen-komponen yang diperlukan:

- struktur record database
- rincian Pengolahan
- teknik kontrol spesifik
- Format untuk layar input dan dokumen sumber
- format laporan outputDesain lakukan, bagaimanapun, memiliki detail yang cukup untuk menunjukkan bagaimana dua sistem secara konseptual berbeda dalam fungsi mereka. Untuk menggambarkan, mari kita memeriksa fitur umum dari setiap sistem.

Opsi A adalah sistem pembelian batch yang tradisional. Input awal untuk proses ini adalah permintaan pembelian dari pengendalian persediaan. Ketika persediaan mencapai titik pemesanan ulang yang telah ditentukan mereka, persediaan baru diperintahkan sesuai dengan jumlah pesanan ekonomi mereka. Pengiriman dari pesanan pembelian kepada pemasok berlangsung sekali sehari melalui surat AS.

Sebaliknya, Pilihan B menggunakan teknologi EDI. Pemicu sistem ini adalah permintaan pembelian dari perencanaan produksi. Sistem pembelian menentukan kuantitas dan vendor dan kemudian mengirimkan pesanan online melalui perangkat lunak EDI ke vendor.

Kedua alternatif memiliki pro dan kontra. Manfaat dari Opsi A adalah kesederhanaan desain, kemudahan implementasi, dan permintaan yang lebih rendah untuk sumber daya sistem dari Option B.Di satu sisi, aspek negatif dari Opsi A adalah bahwa ia memerlukan perusahaan untuk membawa persediaan. Di sisi lain, Pilihan B

memungkinkan perusahaan untuk mengurangi atau bahkan menghilangkan persediaan. Manfaat ini datang pada biaya sumber daya lebih mahal dan canggih sistem. Ini adalah prematur, pada titik ini, untuk mencoba untuk mengevaluasi manfaat relatif dari alternatif ini. Hal ini dilakukan secara resmi di tahap berikutnya dalam SDLC. Pada titik ini, perancang sistem yang bersangkutan hanya dengan mengidentifikasi desain sistem yang masuk akal.

b. Pendekatan Berorientasi Objek
   Desain berorientasi objek (OOD) pendekatan adalah untuk membangun sistem informasi dari komponen standar dapat digunakan kembali atau benda. Pendekatan ini dapat disamakan dengan proses membangun sebuah mobil.
c. Peran Auditor dalam Desain Sistem KonseptualAuditor adalah pemangku kepentingan di semua sistem keuangan dan, dengan demikian, memiliki minat dalam tahap desain konseptual dari sistem. The auditability dari sistem sebagian bergantung pada karakteristik desain. Beberapa teknik audit komputer memerlukan sistem yang akan dirancang dengan fitur audit khusus yang merupakan bagian integral sistem. Fitur Audit ini harus ditentukan pada tahap desain konseptual.

4. Sistem Evaluasi dan Seleksi - Tahap 4

Tahap berikutnya dalam SDLC adalah prosedur untuk memilih salah satu sistem dari himpunanalternatif desain konseptual yang akan pergi ke tahap desain rinci. Evaluasi sistem dan seleksi fase adalah proses optimasi yang berusaha untuk mengidentifikasi sistem yang terbaik. Keputusan ini merupakan saat yang kritis dalam SDLC. Pada titik ini, ada banyak ketidakpastian tentang sistem, dan keputusan yang buruk di sini bisa menjadi bencana. Tujuan dari evaluasi dan seleksi prosedur formal adalah struktur proses pengambilan keputusan ini dan dengan demikian mengurangi ketidakpastian baik dan risiko membuat keputusan yang buruk.

a. Lakukan Detil Studi Kelayakan
   1) Kelayakan Teknis.
   2) Kelayakan Ekonomi.
   3) Kelayakan Hukum.
   4) Kelayakan Operasional.
   5) Jadwal Kelayakan.
b. Melakukan Analisis Biaya-Manfaat

Ada tiga langkah dalam penerapan analisis biaya-manfaat: mengidentifikasi biaya, identifikasi manfaat, dan membandingkan biaya dan manfaat. Kami membahas setiap langkah di bawah ini.

1) Mengidentifikasi Biaya.
    a) Satu Biaya Waktu
        - akuisisi Hardware
        - Persiapan lokasi
        - Akuisisi Software
        - Desain Sistem
        - Pemrograman dan pengujian
        - Data konversi dari sistem lama ke sistem baru
        - Pelatihan Personil
    b) Biaya Reccurring
        - Pemeliharaan Hardware
        - Kontrak pemeliharaan Software
        - Asuransi
        - Persediaan
        - Personil
2) Mengidentifikasi Manfaat
    a) Manfaat Tangible
        - Peningkatan Pendapatan
            - ✓ Peningkatan penjualan dalam pasar yang ada
            - ✓ Ekspansi ke pasar lain
        - Pengurangan biaya
            - ✓ pengurangan tenaga kerja
            - ✓ pengurangan biaya operasi (seperti persediaan dan overhead)
            - ✓ Mengurangi persediaan
            - ✓ Peralatan yang lebih murah
            - ✓ Mengurangi Pemeliharaan peralatan
    b) Manfaat Tak Berwujud
        - ✓ Peningkatan kepuasan pelanggan
        - ✓ Peningkatan kepuasan karyawan
        - ✓ Informasi lebih lanjut saat ini
        - ✓ Peningkatan pengambilan keputusan
        - ✓ Respon cepat terhadap tindakan pesaing
        - ✓ Operasi yang lebih efisien
        - ✓ Komunikasi internal dan eksternal yang lebih baik
        - ✓ Peningkatan perencanaan

- ✓ Fleksibilitas Operasional
- ✓ Peningkatan lingkungan pengendalian

3) Bandingkan Biaya dan Manfaat
   a) Metode Nilai kini
      Nilai sekarang dari biaya dikurangi dari nilai sekarang dari manfaat sepanjang umur sistem.
   b) Metode Payback
      Metode payback adalah variasi dari analisis impas. Break-even point tercapai bila biaya total sama dengan total manfaat.

c. Siapkan Sistem Seleksi Laporan
   Produk penyampaian dari proses seleksi sistem adalah laporan seleksi sistem. Dokumen formal ini terdiri dari studi kelayakan direvisi, analisis biaya-manfaat, dan daftar dan penjelasan manfaat tak berwujud untuk setiap desain alternatif. Atas dasar laporan ini, komite pengarah akan memilih satu sistem yang akan maju ke tahap berikutnya dari desain SDLC-rinci.

d. Peran Auditor dalam Evaluasi dan Seleksi
   Perhatian utama bagi auditor adalah bahwa kelayakan ekonomi dari sistem yang diusulkan diukur seakurat mungkin. Secara khusus, auditor harus memastikan lima hal:
   1) Hanya biaya escapable digunakan dalam perhitungan manfaat penghematan biaya.
   2) suku bunga wajar yang digunakan dalam mengukur nilai sekarang dari arus kas.
   3) Satu-waktu dan biaya berulang yang lengkap dan akurat dilaporkan.
   4) kehidupan Realistis berguna digunakan dalam membandingkan proyek bersaing.
   5) manfaat tidak berwujud ditugaskan nilai keuangan yang wajar.

   Kesalahan, kelalaian, dan kekeliruan dalam akuntansi untuk item tersebut dapat mengganggu analisis dan dapat menghasilkan keputusan material cacat.

5. Detil Desain - Fase 5

Tujuan dari tahap desain rinci adalah untuk menghasilkan penjelasan rinci tentang pro yangsistem yang baik memenuhi persyaratan sistem yang diidentifikasi selama analisis sistem dan sesuai dengan desain konseptual yang diajukan. Pada fase ini, semua komponen sistem (tampilan pengguna, tabel database, proses, dan kontrol) yang cermat ditentukan.

a. Melakukan Desain Sistem Walkthrough
   Setelah menyelesaikan desain rinci, tim pengembangan biasanya melakukan walkthrough desain sistem untuk memastikan bahwa desain bebas dari kesalahan konseptual yang bisa menjadi diprogram ke dalam sistem final. Banyak perusahaan

memiliki formal, walkthrough terstruktur yang dilakukan oleh sekelompok jaminan kualitas. Kelompok ini merupakan salah satu independen yang terdiri dari programmer, analis, pengguna, dan auditor internal. Tugas kelompok ini adalah untuk mensimulasikan pengoperasian sistem untuk mengungkap kesalahan, kelalaian, dan ambiguitas dalam desain. Kebanyakan kesalahan sistem berasal dari desain miskin daripada kesalahan pemrograman. Mendeteksi dan mengoreksi kesalahan dalam tahap desain sehingga mengurangi pemrograman ulang mahal nanti.

b. Dokumentasi Ulasan Sistem

Rinci dokumen laporan desain dan menjelaskan sistem ke titik ini. IniLaporan meliputi:

- Desain untuk semua masukan layar dan dokumen sumber untuk sistem.
- Desain dari semua output layar, laporan, dan dokumen operasional.
- Data Normalisasi untuk tabel database, menentukan semua elemen data.
- Struktur database dan diagram: hubungan Entity (ER) diagram yang menggambarkan hubungan data dalam sistem, diagram konteks untuk sistem secara keseluruhan, data flow diagram tingkat rendah dari proses sistem tertentu, diagram struktur untuk modul program dalam sistem-termasuk termasuk deskripsi pseudocode dari setiap modul.
- Logika Pengolahan (flow chart).

6. Application Programming dan Pengujian - Tahap 6

a. Program Software AplikasiTahap berikutnya dari SDLC adalah untuk memilih bahasa pemrograman dari antara berbagai bahasa yang tersedia dan cocok untuk aplikasi. Ini termasuk bahasa prosedural seperti COBOL, bahasa-event seperti Visual Basic, atau pemrograman berorientasi objek (OOP) bahasa seperti Java atau C ++. Bagian ini menyajikan gambaran singkat dari berbagai pendekatan pemrograman. Sistem profesional akan membuat keputusan mereka berdasarkan in-house standar, arsitektur, dan kebutuhan pengguna.

   1) Bahasa prosedural.
   2) Kegiatan-Driven Bahasa.
   3) Berorientasi Objek Bahasa
   4) Pemrograman Sistem.
      a) efisiensi Programming.
      b) efisiensi Pemeliharaan
      c) Pengendalian

b. Menguji Software Aplikasi

Semua modul program harus diuji secara menyeluruh sebelum mereka diimplementasikan. Ada beberapa konsep terbukti tentang pengujian yang harus diikuti oleh para pengembang sistem, dan dianggap oleh auditor dalam melakukan audit.

1) Pengujian Metodologi
2) Pengujian Offline Sebelum Menyebarkan Online.
3) Data Uji

7. Implementasi Sistem - Tahap 7

Pada tahap implementasi sistem dari proses pengembangan sistem, struktur database yang dibuat dan diisi dengan data, peralatan yang dibeli dan diinstal, karyawan dilatih, sistem didokumentasikan, dan sistem baru dipasang. Proses pelaksanaan melibatkan upaya desainer, programmer, database administrator, pengguna, dan akuntan. Kegiatan dalam tahap ini memerlukan biaya yang luas dan akan sering mengkonsumsi lebih banyak tenaga-jam dari semua tahapan pelaksanaan pra lain dari SDLC gabungan.

a. Menguji seluruh sistem

Ketika semua modul telah dikodekan dan diuji, mereka harus dibawa bersama-sama dan diuji secara keseluruhan. Personil pengguna harus mengarahkan pengujian seluruh sistem sebagai awal untuk implementasi sistem formal. Prosedur ini melibatkan mengolah data hipotetis melalui sistem. Output dari sistem tersebut kemudian berdamai dengan hasil yang telah ditentukan, dan tes didokumentasikan untuk memberikan bukti kinerja sistem. Akhirnya, ketika mereka melakukan tes puas dengan hasilnya, mereka harus kemudian menyelesaikan dokumen penerimaan formal. Ini merupakan pengakuan eksplisit oleh pengguna bahwa sistem tersebut Anda memenuhi persyaratan dinyatakan. Dokumen penerimaan pengguna menjadi penting dalam mendamaikan perbedaan dan menugaskan tanggung jawab selama pemeriksaan pasca implementasi sistem.

b. Mendokumentasikan Sistem

Dokumentasi sistem menyediakan auditor dengan informasi penting tentang bagaimana sistem bekerja. Persyaratan dokumentasi tiga kelompok-sistem desainer dan programmer, operator komputer, dan pengguna akhir-sangat penting tertentu.

1) Designer dan Programmer Dokumentasi.
2) Dokumentasi Operator.
    a) Nama dari sistem, seperti Pembelian Sistem
    b) Jadwal run (harian, mingguan, waktu hari, dan sebagainya)
    c) Perangkat keras yang diperlukan (kaset, disk, printer, atau perangkat keras khusus)
    d) Persyaratan berkas menentukan semua transaksi (input) file, file induk, dan file output yang digunakan dalam sistem diambil, dan nama dan nomor telepon dari programmer on call, harus sistem gagal
    e) Daftar pengguna yang menerima output dari menjalankan
3) Dokumentasi Pengguna.
    a) Siswa

b) Pengguna Sesekali
c) Pengguna cahaya Sering
d) Pengguna listrik yang sering

4) Handbook Pengguna.

Buku pegangan pengguna biasa akan berisi item berikut:

a) Gambaran dari sistem dan fungsi utama
b) Instruksi untuk memulai
c) Deskripsi prosedur dengan langkah-demi-langkah referensi visual
d) Contoh layar masukan dan petunjuk untuk memasukkan data
e) Sebuah daftar lengkap kode pesan kesalahan dan deskripsi
f) Sebuah panduan referensi perintah untuk menjalankan sistem
g) Sebuah daftar istilah kuncih) Layanan dan dukungan informasi

5) Tutorial
6) Fitur Bantuan

c. Mengkonversi Database

Konversi database merupakan langkah penting dalam tahap implementasi. Ini adalah transfer data dari bentuk yang sekarang ke format atau media yang diperlukan oleh sistem baru. Dalam kasus apapun, konversi data adalah berisiko dan harus dikendalikan dengan hati-hati. Tindakan pencegahan berikut harus diambil:

1) Validasi
2) Rekonsiliasi
3) Backup

d. Konversi ke Sistem Baru

Proses konversi dari sistem lama ke yang baru disebut cutover tersebut. Sebuah sistem cutover biasanya akan mengikuti salah satu dari tiga pendekatan: kalkun dingin, bertahap, atauoperasi paralel.

1) Cold Turkey cutover
2) Bertahap cutover
3) Paralel cutover Operasi

e. Peran Auditor dalam Pelaksanaan Sistem

Auditor eksternal dilarang oleh undang-undang SOX dari keterlibatan langsung dalam pelaksanaan sistem. Namun, seperti pembahasan sebelumnya telah menyarankan, peran auditor internal dalam desain dan pelaksanaan tahapan rinci harus signifikan. Menjadi pemangku kepentingan di semua sistem keuangan, auditor internal harus meminjamkan keahlian mereka untuk proses ini untuk membimbing dan membentuk sistem selesai. Secara khusus, auditor internal dapat terlibat dengan cara berikut.

1) Memberikan Keahlian Teknis.
2) Tentukan Standar Dokumentasi.

3) Verifikasi Pengendalian Kecukupan dan Kepatuhan SOX

f. Post-Implementasi Ulasan

Salah satu langkah yang paling penting dalam tahap implementasi sebenarnya berlangsung beberapa bulan kemudian di review pasca implementasi. Ulasan ini dilakukan oleh tim independen untuk mengukur keberhasilan sistem dan proses setelah debu telah melunasi.

1) Desain Sistem Adequacy

Ciri-ciri fisik dari sistem harus ditinjau untuk melihat apakah mereka memenuhi kebutuhan pengguna. Resensi harus mencari jawaban jenis berikut pertanyaan:

a) Apakah output dari sistem memiliki karakteristik seperti informasi sebagai relevansi, ketepatan waktu, kelengkapan, akurasi, dan sebagainya? grafik, elektronik, hard copy, dan sebagainya)?
b) Apakah data yang hilang, rusak, atau digandakan oleh proses konversi?
c) Apakah bentuk input dan layar dirancang dan kebutuhan pengguna pertemuan?
d) Apakah pengguna menggunakan sistem dengan benar?
e) Apakah pengolahan tampaknya benar?
f) Dapatkah semua modul program diakses dan dieksekusi dengan baik, atau apakah pengguna yang pernah terjebak dalam satu lingkaran?
g) Apakah sistem menyediakan pengguna bantuan dan tutorial yang memadai?

2) Akurasi Waktu, Perkiraan Biaya, dan Manfaat

Tugas memperkirakan waktu, biaya, dan manfaat bagi sistem yang diusulkan adalah rumit oleh ketidakpastian. Hal ini terutama berlaku untuk proyek-proyek besar yang melibatkan banyak kegiatan dan kerangka waktu yang lama. Semakin variabel dalam proses, semakin besar kemungkinan untuk kesalahan material dalam perkiraan. Sejarah sering guru terbaik untuk keputusan semacam ini. Oleh karena itu, review kinerja aktual dibandingkan dengan jumlah yang dianggarkan memberikan masukan penting untuk penganggaran masa depankeputusan. Dari informasi tersebut, kita dapat belajar di mana kesalahan yang dibuat dan bagaimana untuk menghindari mereka waktu berikutnya. Pertanyaan-pertanyaan berikut memberikan beberapa wawasan:

a) Apakah biaya yang sebenarnya sejalan dengan biaya yang dianggarkan?
b) Apa bidang keberangkatan yang signifikan dari anggaran?
c) Apakah keberangkatan dari anggaran terkendali (internal) dalam jangka pendek atau non dikontrol (misalnya, masalah pemasok)?
d) Apakah tingkat pengerjaan ulang karena desain dan coding kesalahan diterima?
e) Apakah pengguna menerima manfaat yang diharapkan dari sistem?

f) Apakah nilai-nilai ditugaskan untuk nyata dan, terutama, manfaat intangible akurat?

8. Pemeliharaan Sistem - Tahap 8

Sistem pemeliharaan adalah proses formal di mana program aplikasi mengalami perubahan untuk mengakomodasi perubahan kebutuhan pengguna. Beberapa perubahan aplikasi yang sepele, seperti memodifikasi sistem untuk menghasilkan laporan baru atau mengubah panjang dari data lapangan. Pemeliharaan juga bisa ekstensif, seperti membuat perubahan besar untuk logika aplikasi dan user interface. Tergantung pada organisasi, periode sistem pemeliharaan dapat bertahan 5 tahun atau lebih. Sistem dalam lingkungan bisnis yang sangat kompetitif melihat jauh lebih pendek sistem masa hidup. Ketika itu tidak layak lagi bagi organisasi untuk terus mempertahankan sistem penuaan, itu dibatalkan, dan siklus hidup pengembangan sistem baru dimulai.

Pemeliharaan merupakan pengeluaran sumber daya yang signifikan dibandingkan dengan biaya pengembangan awal. Selama masa hidup sistem, sebanyak 80 sampai 90 persen dari total biaya yang mungkin timbul dalam tahap pemeliharaan. Kami meninjau implikasi audit pemeliharaan di bagian berikutnya.

C. PENGENDALIAN DAN AUDIT ATAS SDLC

a. Mengontrol Pengembangan Sistem Baru

a. Sistem Otorisasi Kegiatan
b. Spesifikasi pengguna Aktivitas
c. Desain Teknis Kegiatan
d. Partisipasi Internal Audit
e. Uji pengguna dan Prosedur Penerimaan
f. Audit Tujuan Terkait Pengembangan Sistem Baru

b. Pengendalian Sistem Pemeliharaan

a. Pemeliharaan Otorisasi, Pengujian, dan Dokumentasi
b. Perpustakaan Program sumber Kontrol
c. The Worst-Case Situasi: Tidak ada Kontrol
d. Sebuah Terkendali SPL Lingkungan
e. Audit Tujuan Terkait Pemeliharaan Sistem
f. Audit Prosedur Terkait Pemeliharaan Sistem

Nama : Caesario Rian Saputra

Nim : 182420131

Kelas : MTIB

Proses Control (Pengendalian)

Tujuan utama dari auditor melakukan audit atas Pengendalian Umum atau Pengendalian Manajemen adalah untuk mengevaluasi kerangka kerja dari aspek-aspek pengendalian umum (Ron Weber lebih menyukai menyebutkan management control) dari TI apakah sudah dilakukan dengan baik oleh manajemen atau belum.

Berikut ini merupakan tindakan yang perlu dilaksanakan dalam pengendalian

1. **Top Management**
   Tujuan utama dari auditor melakukan audit atas Pengendalian Umum atau Pengendalian Manajemen adalah untuk mengevaluasi kerangka kerja dari aspek-aspek pengendalian umum (Ron Weber lebih menyukai menyebutkan management control) dari TI apakah sudah dilakukan dengan baik oleh manajemen atau belum.
2. **IS Managament**
   bertanggung jawab secara keseluruhan atas perencanaan dan pengendalian kegiatan dan aktivitas sistem informasi. Selain itu, berkewajiban untuk memberikan masukan kepada manajemen puncak berkaitan dengan penyusunan kebijakan jangka panjang dan menerjemahkannya ke dalam rencana tujuan dan sasaran jangka pendek.
3. **System Development Management**
   bertanggung jawab atas desain, implementasi dan pemeliharaan sistem aplikasi.
4. **Programming Management**
   bertanggung jawab atas pemrograman sistem yang baru, memelihara sistem yang lama dan menyediakan perangkat lunak dukungan sistem.
5. **Data Managament**
   bertanggung jawab untuk membuat perencanaan dan penyesuaian isu-isu pengendalian yang berkaitan dengan penggunaan data organisasi.
6. **Quality Assurance Management**
   bertanggung jawab atas pengendalian akses dan pengamanan fisik untuk sumber daya teknologi informasi.
7. **Operation Management**
   bertanggung jawab untuk memastikan bahwa pengembangan, implementasi, operasionalisasi dan pemeliharaan sistem informasi sesuai dengan standar kualitas yang sudah ditetapkan.
8. **Application System Control**
   bertanggung jawab atas perencanaan dan pengendalian operasional harian teknologi informasi

Nama : Dhea Noranita Putri
NIM : 182420112 (MTI REG B 2019)
Tugas : IT Audit
Tanggal : 2 April 2020

SOAL

untuk proses control (pengendalian) ada tindakan yang perlu dilaksanakan, gunaka referensi yang ada untuk menjawap pertanyaan saya tertutama dalam hal pengembangan sistem, pemrogramaan dan operasional

JAWAB

Proses pengendalian dan tindakan yang perlu dilaksanakan dalam pengembangan system, program dan operasional. **Pengembangan system** auditor terlibat dalam memberikan argument karna pada tahap ini auditor berperan memberikan solusi terhadap permasalahaan saat ini. Terdapat 3 yaitu :

1. **Concurrent audit** adalah auditor menjadi anggota dalam tim pengembangan sistem (system development team). Mereka membantu tim untuk meningkatkan kualitas pengembangan sistem yang dibangun oleh para sistem analis, designer dan programmer dan akan diimplementasikan.
2. **Post implementation Audit**, dilakukan setelah tahap pengembangan telah selesai dilakukan. Tujuannya untuk memeriksa apakah sistem-sistem aplikasi komputer yang telah diimplementasikan pada suatu organisasi/perusahaan telah sesuai dengan kebutuhan penggunanya (efektif) dan telah dijalankan dengan sumber daya optimal (efisien). Auditor mengevaluasi apakah sistem aplikasi tertentu dapat terus dilanjutkan karena sudah berjalan baik dan sesuai dengan kebutuhan usernya atau perlu dimodifikasi dan bahkan perlu dihentikan.
3. **General Audit,** Auditor melakukan penilaian terhadap pengendalian atas pengembangan system secara keseluaruan. auditor mengevaluasi kinerja unit fngsional atau fungsi sistem informasi (pusat/instalasi komputer) apakah telah dikelola dengan baik, apakah kontrol dalam pengembangan sistem secara keseluruhan sudah dilakukan dengan baik, apakah sistem komputer telah dikelola dan dioperasikan dengan baik.

Dalam mengaudit sistem komputerisasi yang ada, audit ini dilakukan dengan mengevaluasi pengendalian umum dari sistem-sistem komputerisasi yang sudah diimplementasikan pada perusahaan tersebut secara keseluruhan. Terdapat 3 manajemen perubahan yaitu :

- **Unfreezing the organization**, yaitu mempersiapkan perubahan dalam perusahaan
- **Moving organization**, yaitu berubah system yang baru
- **Refreezing the organization**, yaitu membantu anggota organisasi yang termasuk dalam system ini, untuk beradaptasi dengan system yang baru.

Poin pengamatan yang auditor pada proses ini ialah :

1. **Studi Kelayakan**, yaitu auditor menentukan hal apa saja yang berubah, apakah dapat dilakukan perubahan dan dipelajari secara cost effective.
2. **Analisa system yang ada**, menganalisa system saat ini dengan mempelajari latar belakang, struktur organisasi dan budaya organisasi ini penting untuk diimplementasikan ke system yang baru.
3. **Menyusun Kebutuhan Strategis**, auditor dalam hal menyusun kebutuhan strategis harus sesuai dengan tujuan dari system.
4. **Mendesain Organisasi dan Pekerjaan**, dalam beberapa kasus untuk mencapai kebutuhan strategis, auditor harus mendesai ulang organisasi dan pekerjaan.
5. **Mendesain Sistem Pemrosesan Informasi**, dalam mengevaluasi fase desain pemerosesan informasi auditor harus memeriksa enam aktivitas utama yaitu, apakah desainer system telah melakukan deskripsi kebutuhan strategis yang diperlukan, auditor telah memastikan aliran data yang menghasilkan informasi, auditor telah memastikan telah menentukan ruang lingkup database, auditor telah memastikan apakan userinterface sudah sesuai standar user interface yang baik, dalam fase physical design auditor memastikan apakah gambaran fisikal design sudah cukup baik atau tidak, selanjutnya auditor harus memastikan apakah desain yang dibuat bisa terintegrasi dengan baik dengan hardware dan software yang ada.
6. **Akusisi / Pengembangan Aplikasi**, setelah mendesain system pemerosesan informasi selanjutnya melakukan request for proposal (RFP) dan evaluasi proposal akan ditekankan pada tahap ini. auditor harus memastikan apakah kemampuan aplikasi yang dibuat sudah sesuai dengan kebutuhan dan berfungsi dengan baik, sehingga prosedur dalam desain, koding, komplikasi, testing dan dokumentasi harus dievaluasi oleh auditor.
7. **Akusisi Perangkat Keras dan Lunak**, dalam hal ini auditor harus mampu meyakinkan bahwa proposal tersebut sudah dipersiapkan dengan baik.
8. **Pengembangan Prosedur,** Pada tahap ini ditentukan aktifitas apa saja yang dilakukan user, tugas auditor ialah menentukan kualitas prosedur tersebut dengan baik.
9. **Uji Penerimaan,** Tujuan dari uji penerimaan adalah untuk mengidentifikasi apakah ada masalah dan penyimpangan dalam proses menuju final.
10. **Konversi dan Implementasi,** pada fase ini maka aktivitas yang bertujuan menempatkan system baru, auditor perlu memperhatikan apakah ada yang belum terindentifikasi,dan konversi dapat menjadi hal yang tidak bersahabat dan user akan menganggap pendekata yang dilakukan selama ini tidak baik

Nama : Dhea Noranita Putri
NIM : 182420112 (MTI REG B 2019)
Tugas : IT Audit
Tanggal : 2 April 2020

11. **Operasi dan Pemeliharaan,** perhatian auditor terhadap hal ini ialah mencatat aktivitas pemeliharaan, perubahan karna aktivitas pemeliharaan dan pengendalian terhadap perubahgan tersebut

Selanjutnya **Manajemen pemograman**, auditor harus memahami karateristik program yang berkualitas tinggi, yaitu berfungsi secara benar dan lengkap, mempunyai interface pengguna yang berkualitas tinggi, bekerja secara efektif, dan mudah dipelihara. Evaluasi pada manajemen pemograman yaitu :

1. **Tahap Perencanaan**, tahap ini sulit dilakukan seorang auditor sebaiknya mengetahui tehnik perkiraan biaya pemograman.
2. **Tahap Desain**, tahap ini auditor diharapkan mengetahui secara umum alasan programmer mengapa programmer menggunakan pendekatan itu. seperti programer mengunakan COBOL, auditor harus memastikan mengapa programer mengunakan hal tersebut.
3. **Tahap Coding**, pada tahap ini programer melakukan penulisan program.
4. **Tahap Testing**, tahap ini ditujukan untuk mengidentifikasi adanya kesalaahan. peran auditor disini iala untuk melihat apakah semuanya telah berjalan dengan baik atau belum. kalau belum tindakan apa yang perlu dilakukan untuk mengatasinya.
5. **Tahap Operasi dan pemeliharaan**, pada tahap ini hal yang perlu di evaluasi auditor adalah monitoring kenerja dan jenis - jenis pemeliharaan dan perbaikan yang dilakukan

Manajemen Operasi Pengendalian ini menentukan apakah fungsi manusia atau operasi otomatis yang harus dilakukan. jenis -jenis operasi tersebut iala operasi normal dari komputer. ketika semakin banyak operasi komputer dilakukan secara terotomatos. auditor harus melakukan pemeriksaan pada masalah -masalah authentifikasi, akurasi dan kelengkapan dari program yang berjalan terotomatis tersebut.

Nama : DINI RAHMADIA
NIM : 182420134 MTI REG B

Tugas : IT AUDIT
Tanggal : 5 April 2020

SOAL

Untuk proses control (pengendalian) ada tindakan yang perlu dilaksanakan, gunakan referensi yang ada untuk menjawab pertanyaan saya terutama dalam hal pengembangan sistem, pemrogramaan dan operasional

JAWABAN

A. PENGEMBANGAN SISTEM

Manajemen pengembangan sistem mempunyai tanggung jawab terhadap proses penganalisaan, perancangan, pembangunan, penerapan, dan pemeliharaan sistem informasi adapun tiga cara pendekatan berbeda untuk audit: sebagai pelaku di dalam proses pengembangan sistem (Concurrent Audit), sebagai reviewer pasca implementasi suatu sistem aplikasi spesifik (Postimplementation Audit), atau reviewer proses pengembangan sistem secara umum (General Audit).

a. **Concurent Audit** : auditor sebagai anggota tim pengembangan sistem. Mereka membatu tim dalam meningkatkan kualitas pengembangan sistem untuk pembangunan dan pengimplementasian sistem spesifik
b. **Postimplementation Audit** : auditor mencari untuk membantu organisasi belajar dari pengalaman dalam pengembangan sistem aplikasi yang spesifik. Tambahan, mereka boleh juga melakukan evaluasi kebutuhan sistem untuk di susun kembali, dilanjutkan atau di modifikasi dalam berbagai cara.
c. **General Audit** : auditor mengevaluasi pengendalian pengembangan sistem secara menyeluruh.

1. EVALUASI TERHADAP PENGEMBANGAN SISTEM

Kualitas pengembangan sistem akan bergantung pada bagaimana keterlibatan (tanggapan) stakeholder terhadap proyek pengembangan sistem yang sedang ditangani. Jika Auditor mengambil bagian dalam proses pengembangan sistem, mereka akan merupakan bagian dari pertimbangan pengambilan keputusan kelompok stakeholder tentang pengarahan terbaik terhadap isu-isu yang ada bagi pengembangan sistem. Jika, pada sisi lain, mereka melaksanakan juga tinjauan ulang (ex post view) terhadap sistem yang spesifik atau proses pengembangan sistem secara umum, mereka akan mengevaluasi bagaimana stakeholder mengarahkan isu-isu yang ada tersebut dan bagaimana pengaruhnya setelah sistem di kembangkan

Tujuannya yaitu stakeholder harus mencoba terbuka untuk memahami bersama persoalan atau kesempatan yang ingin diraih. Adalah peluang atau kesempatan yang baik atau tidak?, mempunyai implikasi kecil atau besar terhadap personal?, Akankah solusi mempunyai dampak yang besar pada struktur organisasi dan job?, Akankah teknologi baru hampir dapat dipastikan dibutuhkan untuk mendukung solusi yang mungkin?.

2. MANAJEMEN PERUBAHAN

Adapun aktivitas yang akan dilakukan manajemen perubahan adalah sebagai berikut;

1. Unfreezing the Organization : menyiapkan organisasi untuk perubahan.
2. Moving the Organization : perubahan sistem kerja untuk sistem baru

3. Refreezing the Organization : membantu user untuk menyesuaikan dengan sistem baru.

3. PENILAIAN KELAYAKAN DAN MASUKAN

Tujuan dari fase penilaian kelayakan dan masukan adalah untuk memperoleh komitmen perubahan dan mengevaluasi apakah solusi penghematan biaya memungkinkan untuk mengarahkan peluang dan tantangan yang sudah berhasil di identifikasi. untuk mengevaluasi kelayakan sistem baru menggunakan empat kriteria yaitu;

1. Kelayakan Teknik (Technical Feasibility)
2. Kelayakan Operasional (Operational Feasibility)
3. Kelayakan Ekonomi (Economic Feasibility)
4. Kelayakan Perilaku (behavioral feasibility)

4. ANALISIS SISTEM YANG SEDANG BERJALAN (EXISTING SYSTEM)

Ketika sistem baru diajukan, dalam beberapa kasus ia akan menggantikan system yang sedang berjalan. Tenaga / fikiran Perancang dibutuhkan untuk memahami sistem yang sedang berjalan (existing system). Jika mereka menghendaki untuk melaksanakan pekerjaan dengan kualitas yang tinggi (baik) dalam pengembangan dan pengimplementasian sistem yang baru

5. SUSUNAN KEBUTUHAN STRATEGIS

Kebutuhan strategis untuk sebuah sistem yang spesifik secara keseluruhan sasaran dan tujuan sistemnya harus terpenuhi. Biasanya mungkin masih kurang jelas, sebagai contoh “meningkatkan kekayaan pemegang saham” atau yang lebih spesific, “mengurangi utasi staff di bagian penjualan sebesar 30%”. Kebutuhan strategis adalah dasar identifikasi untuk memahami sistem yang ada atau memahami peluang untuk meningkatkan kinerja tugas dan kualitas pekerjaan.

6. ORGANISASI DAN RANCANGAN JOB

Dalam beberapa kasus, penyelesaian pilihan kebutuhan strategis untuk sistem akan memerlukan rancangan awal (initial design) atau rancangan ulang (redesign) struktur organisasi dan job.

Dalam pemilihan struktur organisasi dan rancangan job suatu bagian organisasi akan efektif melalui usulan pengajuan sistem, banyak faktor yang dapat dipertimbangkan.

7. DESAIN SISTEM PENGOLAHAN INFORMASI

Ketika mengevaluasi fase desain sistem pengolahan informasi, salah satu dari partisipan dalam proses desain atau dalam postimplementation atau meneliti kapasitas secara mum, maka auditor harus memerika enam aktivitas utama yaitu :

1. Memunculkan kebutuhan secara detil (elicitation of detailed requirements) 2. Desain aliran data / informasi (design of the data / information flow) 3. Desain database (design of the database) 4. Desain hubungan dengan user (design of the user interface) 5. Desain fisik (physical design) dan 6. Desain dan akuisisi hardware dan platform system software (design and acquisition of the hardware / system software platform

8. PENGEMBANGAN DAN PENGADAAN SOFTWARE APLIKASI

Auditor harus mempunyai konsentrasi selama akuisisi dan fase pengembangan. Jika aplikasi s/w terakuisisi, mereka akan konsen tentang pemenuhan spesifikasi kebutuhan yang disediakan untuk vendor, kualitas prosedur yang digunakan untuk mengevaluasI

9. OPERASIONAL DAN PEMELIHARAAN

Selama fase operasional dan pemeliharaan, sistem baru dijalankan sebagai produk dari sistem. Pemeliharaan mencakup : 1. Repair Maintenance (pemeliharaan perbaikan) 2. Adaptive Maintenance dan (pemeliharaan penyesuaian) 3. Perfective maintenance (pemeliharaan penyempurnaan)

B. PEMPROGRAMAN SISTEM

Pemrograman merupakan proses dari sistem pengendalian manajemen. Pada saat perusahaan didirikan, pemrograman baru dapat dilakukan setelah tujuan dan strategi pencapaian tujuan tersebut ditentukan. Sebaliknya, setelah perusahaan berjalan realisasi yang efektif dan efisien namun tidak mencapai tujuan perusahaan akan menimbulkan evakuasi terhadap program, strategi atau tujuan perusahaan. Selanjutnya evaluasi tersebut dapat juga menyebabkan perubahan terhadap program, strategi, atau tujuan perusahaan.

1. Evaluasi Program

Pelaksanaan program memerlukan sumberdaya, oleh karena sumberdaya jumlahnya terbatas, maka perlu diadakan seleksi terhadap program yang akan dilaksanakan. Untuk memilih program yang tepat manajemen harus menggunakan teknik-teknik seleksi dalam memilih program yang diawali dengan pengusulan investasi.

Pemrograman yang didasarkan pada tujuan dan strategi perusahaan berdasarkan definisi sistem pengendalian adalah sebuah sistem yang terdiri dari beberapa sub sistem yang saling berkaitan antara pemrograman, penganggaran, akuntansi, pelaporan dan pertanggungjawaban untuk mempengaruhi orang lain. Dalam sebuah perusahaan dalam rangka mencapai tujuan perusahaan melalui strategi tertentu dengan secara efektif dan efisien, hal ini dianggap sudah ditentukan oleh perusahaan. Tujuan dan strategi disusun dengan memperhatikan peluang, ancaman, hambatam, dan kesempatan (analisis SWOT). Berdasarkan tujuan dan strategi yang telah ditetapkan perusahaan, suatu bagian menyusun program untuk mencapai tujuan yang telah ditentukan. Oleh karena program merupakan alokasi sumberdaya jangka panjang. Oleh karena program merupakan alokasi sumberdaya jangka panjang, maka program disebut juga sebagai rencana jangka panjang, melalui penganggaran rencana jangka panjang tersebut kemudian dijabarkan menjadi rencana jangka pendek

2. Tahapan pemprograman

1. Problem Definiton

Problem Definition ialah menjelaskan dan memahami suatu masalah hingga ke akar-akarnya. Kita harus memahami masalah intinya,kebutuhan kita, dan output yang akan kita hasilkan

2. Problem Analys

Problem Analys ialah menganalisis suatu masalah dengan menentukan apa saja yang akan kita gunakan seperti variable,fungsi, dll.

Di Fase ini kita juga memikirkan bagaimana solusi dari permasalahan terebut

3. Algorithm Development

Di fase ini kita menentukan algoritma dalam penyelesaian suatu masalah. Algoritma sendiri ialah kumpulan langkah langkah untuk menyelesaikan suatu masalah. Fase ini merupakan fase paling penting dalam pembuatan suatu program

4. Coding & Documentation

Coding ialah proses penerjemahan algoritma kita ke bahasa pemrograman yang dipahami oleh komputer. Fase ini ialah Proses inti dalam Pemrograman

Dokumentasi sendiri ialah proses penyimpanan suatu algoritma atau coding dalam suatu berkas agar bisa ditinjau di kemudian hari.

5. Testing

Testing ialah proses pengujian apakah suatu program tersebut dapat menyelesaikan masalah kita. Dengan melihat input yang kita masukkan dan output yang kita harapkan

6. Maintenance

Maintenance ialah proses perbaikan jika program tersebut mengalami error dan hal hal yang tidak kita harapkan. Proses Maintenance akan membawa kita kembali ke desain dan pengembangan algoritma.

C. MANAJEMEN OPERASIONAL

Manajemen operasional adalah suatu usaha pengelolaan secara maksimal penggunan semua faktor produksi yang ada baik itu tenaga kerja (SDM), mesin, peralatan, *raw material* (bahan mentah) dan faktor produksi yang lainnya dalam proses tranformasi untuk menjadi berbagai macam produk barang atau jasa.

Nama : DINI RAHMADIA
NIM : 182420134 MTI REG B
Tugas : IT AUDIT
Tanggal : 5 April 2020

Tanggung jawab manajer operasional :

⇐ Menghasilkan barang atau jasa.

⇐ Mengambil sebuah keputusan mengenai fungsi operasi serta sistem transformasi.

⇐ Mengkaji pengambilan sebuah keputusan dari suatu fungsi operasinal.

Fungsi produksi dan operasional

⇐ Proses produksi serta operasional

⇐ Jasa penunjang dalam pelayanan produksi

⇐ Planning (Perencanaan)

⇐ Controlling (Pengendalian dan pengawasan)

Lingkup Manajemen Operasional :

1. Perancangan desain sistem produksi dan operasional

- Seleksi serta perancangan desain produk
- Seleksi serta perancangan proses dan peraalatan
- Pemilihan site dan lokasi perusahaan serta unit produksi
- Rancangan tata letak serta arus kerja
- Rancangan atas tugas pekerjaan
- Strategi produksi dan operasional serta pemilihan kapasitas

2. Pengoperasian sistem produksi dan operasional

- Menyusun rencana produk dan operasional
- Perencanaan dan pengendalian atas persediaan serta pengadaan bahan
- Pemeliharaan utilitas mesin dan juga peralatan
- Pengendalian atas mutu
- Manajemen sumber daya manusia (tenaga kerja)

Nama : **Ekariva Annas Asmara**
NIM : **182420133**
Kelas : **Reguler A**

Control dan Audit TI

Untuk proses control (pengendalian) ada tindakan yang perlu dilaksanakan, gunakan referensi yang ada untuk menjawab pertanyaan saya terutama dalam hal pengembangan sistem, pemrogramaan dan operasional

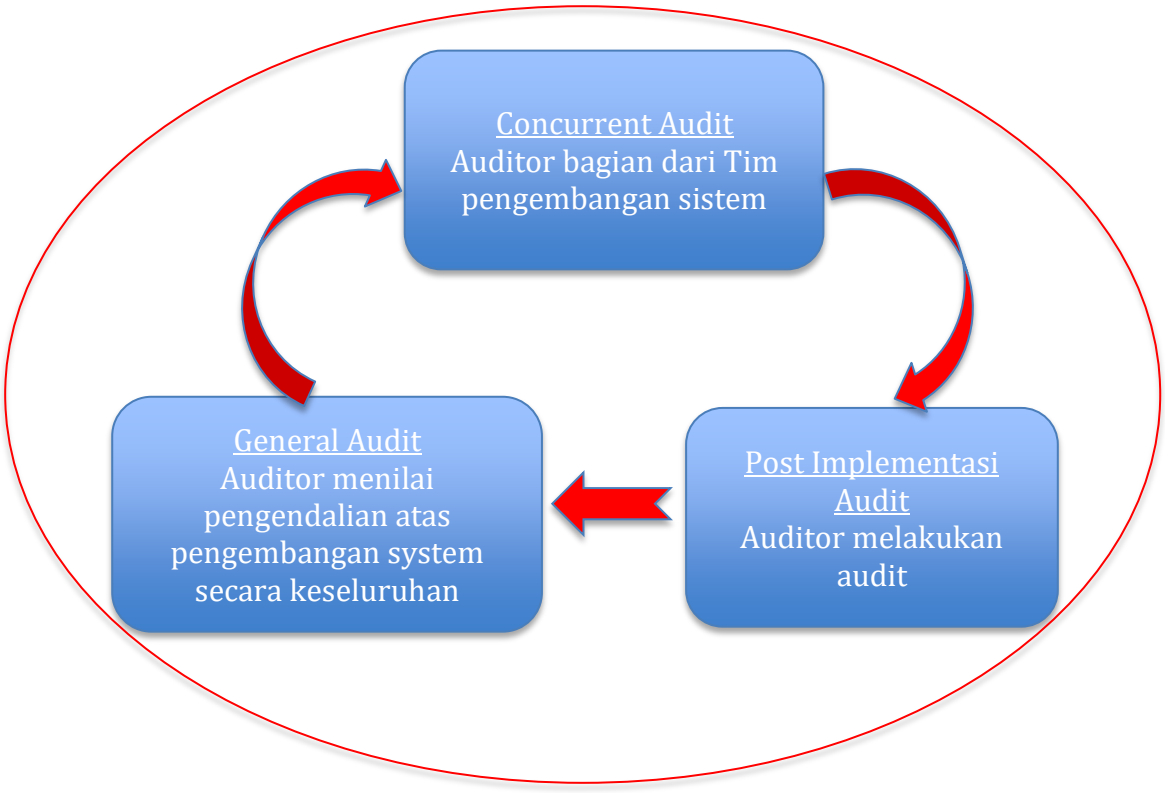
Jawaban :

1. Pengembangan Sistem

   Dalam pengembangan sistem ini sangat perlu dilakukan karena dengan pengembangan sistem jika terjadi kesalahan dapat segera diperbaiki.

   a. Pendekatan Audit atas pengembangan sistem

      Auditor dapat memilih atau dikombinasi dalam melakukan audit atas pengembangan sistem :



b. Evaluasi atas pengembangan sistem

Sistem informasi dibuat untuk mengatasi permasalahan ataupun mengambil keuntungan dari peluang yang ada.

Auditor musti memiliki 4 keingaintahuan, yaitu :

- Apakah kemungkinan penyelesaian sistem informasi akan berdampak dan berpengaruh terhadap perusahaan?jika ya apakah sudah diberitahukan pada seluruh jajaran perusahaan.
- Jika nantinya Sstem Informasi akan merubah jajaran, jajaran mana yang akan diubah
- Jika nanti Sistem Informasi memiliki ketidakpastian mengenai teknologi yang digunakan, apakah sudah ada Tindakan yang akan diambil
- Apakah seluruh perusahaan setuju pada masalah dan peluang yang ada.

Manajemen Perubahan - Manajemen perubahan berjalan bersamaan dengan semua proses dalam pengembangan sistem. Ada tiga (3) aktivitas yang perlu dilakukan perusahaan selama perubahan ini yaitu :

- Unfreezing the organization - yaitu mempersiapkan perubahan dalam perusahaan dengan pendekatan mendidik.
- Moving the organization - yaitu berubah ke sistem yang baru dibuat.
- Refreezing the organization - yaitu menolong siapa saja yang berkaitan dengan sistem ini untuk beradaptasi dan merasa nyaman dengan sistem yang baru ini.

Selama proses ini auditor menitikberatkan pengamatan pada proses transformasi ini. Studi kelayakan - Tujuan dari bagian ini ialah untuk memperoleh komitmen perubahan dari seluruh bagian yang bakal berubah dan mempelajari secara cost-effective apakah perubahan ini masih bisa dilakukan atau tidak. Ada empat (4) studi kelayakan yang perlu dilakukan oleh perusahaan yaitu:

- Technical Feasibility - Apakah tehnologi yang ada saat ini sanggup menjalankan sistem yang akan dibuat? dapatkah tehnologi tersebut dibuat dan dilaksanakan?
- Operational Feasibility - Apakah data yang dimasukkan ke sistem dapat dikumpulkan oleh sistem? Apakah hasilnya keluarannya dapat berguna?

- Economic Feasibility - Apakah biaya pembuatan sistem ini nantinya akan lebih kecil dari manfaat yang akan didapatkan dari sistem ini nantinya?
- Behavioral Feasibility - Dampak apa sajakah yang akan terjadi pada pengguna?

Auditor dalam hal ini untuk memastikan apakah semua studi kelayakan ini mempunyai hasil yang baik karena kalau tidak akan menimbulkan permasalahan di kemudian hari.

Analisa Sistem Yang Ada - Apabila sistem yang baru akan di rekomendasikan untuk menggantikan sistem yang ada. Desainer dari sistem perlu mengetahui sistem yang sudah ada. Ada beberapa hal yang perlu dilakukan oleh perusahaan yaitu:

Mempelajari latar belakang struktur dan budaya organisasi, desainer perlu mempelajari sejarah perusahaan yang sekarang, struktur dan kebudayaan untuk memperoleh pemahaman yang prima. Auditor dalam hal ini menitikberatkan perhatian pada evaluasi keputusan desainer dalam hal (1) apakah mereka perlu mempelajari latar belakang perusahaan; (2) jika ya aspek apa yang perlu dipelajari; dan (3) tingkat kedalaman pemahaman yang perlu dipelajari.

Mempelajari arus produk dan informasi, hal ini penting untuk tiga hal yaitu (1) kadangkala desain dari sistem yang akan diusulkan akan bertumpu pada produk dan aliran informasi sistem yang ada sekarang. (2) desainer perlu mengerti kekuatan dan kelemahan dari produk yang ada. (3) pemahaman yang baik tentang produk yang ada dan aliran informasi akan diperlukan dalam proses implementasi sistem baru. Dalam hal ini auditor akan menitikberatkan perhatian pada tiga hal yaitu (1) harus dievaluasi setiap tanggapan atau reaksi dari stakeholders terhadap setiap usulan sistem, (2) auditor harus memeriksa apakah stakeholders menggunakan metode yang baik dalam menanggapi usulan sistem yang ajukan seperti object oriented analysis, dll. (3) auditor harus memastikan apakah desainer menggunakan alat perancangan yang baik seperti CASE (computer-aided software-engineering) tools untuk mendukung usulan mereka.

Menyusun Kebutuhan Strategis - Kebutuhan strategik yang perlu di penuhi oleh sistem ialah tujuan dari sistem yang kongkrit. Seperti mengurangi tingkat perputaran staf dalam area penjualan sebesar 30 %. Auditor dalam hal ini harus

memusatkan perhatiannya pada apakah desainer dari sistem menyadari betul pentingnya kebutuhan strategik ini.

Mendesain Organisasi dan Pekerjaan - Dalam beberapa kasus, untuk mencapai kebutuhan strategis diperlukan desain atau desain ulang dari struktur organisasi dan pekerjaan. Jika auditor sudah dapat memastikan bahwa langkah ini bukan merupakan masalah lagi, itu berarti auditor dapat mengurangi tingkat resiko pengendalian yang berkaitan dengan pengembangan sistem. Jika tidak maka auditor harus meninjau ulang pendapat mereka tentang resiko pengendalian di bidang ini dan berencana meningkatkan substantive test.

Mendesain Sistem Pemrosesan Informasi - Ketika mengevaluasi fase desain sistem pemrosesan informasi, baik itu sebagai partisipan dalam proses desain atau pun audit setelah implementasi, seorang auditor harus memeriksa enam aktivitas utama yaitu :

- Elicitation of detailed requirements - Dalam bidang ini auditor harus mengevaluasi apakah desainer dari sistem telah melakukan pendeskripsian kebutuhan strategis apa saja yang diperlukan untuk meminimalisir ketidakpastian disekeliling sistem yang diusulkan. Auditor harus memastikan sebaik apa strategi penjelasan ini dikomunikasikan.
- Design of the data/information flow - Kegagalan dalam menghasilkan desain yang baik bagi data/aliran informasi dapat melemahkan sistem. Contohnya kesalahan dalam menentukan aliran data akan menghasilkan informasi yang salah alamat. Auditor harus berhati-hati dalam mengevaluasi fase ini dan memastikan bahwa hasil yang dilakukan oleh sistem ini memang benar-benar seperti yang diharapkan dan sesuai dengan rencana.
- Design of database - Dalam mendesain sebuah database kegiatan yang termasuk di dalamnya ialah mendefinisikan ruang lingkup (konteks) dan struktur. Skope database antara lokal sampai global. Dalam tahap ini auditor harus hati-hati mengevaluasi keputusan dalam ruang lingkup database untuk mendefinisikan apakah hal tersebut masuk akal atau tidak untuk dilaksanakan.
- Design of user interface - Dalam mendesain user interface termasuk kegiatan mendefinisikan cara user berhubungan dengan sistem. Auditor pada umumnya akan menganggap hal ini penting. Karena hal ini berhubungan dengan tingkat

kesalahan yang akan dilakukan oleh user. Auditor harus memastikan apakah desainer sudah mengikuti suatu standar yang barhubungan dengan bagaimana membuat suatu desain interface yang baik.

- Physical design - Pada dasarnya segala sesuatu yang sudah dirancang secara logikal akan di masukkan ke dalam tahap physical desain. Dalam fase ini auditor menitikberatkan perhatian dalam meneliti apakah gambaran fisikal desain sudah cukup baik atau tidak. Karena kalau sembarangan mengambarkannya dan menentukannya akan menghasilkan sistem yang tidak efektif dan efisien.
- Design & acquisition of hardware/system software platform - Jika dalam kasus sistem yang direncanakan akan membutuhkan hardware atau software yang belum pernah dimiliki oleh perusahaan, maka harware atau pun software yang ada harus didesain sendiri. Dalam hal ini auditor harus memastikan agar desain yang dibuat bisa terintegrasi dengan baik dengan hardware atau software yang sudah eksis.

Akuisisi/Pengembangan Aplikasi - Setelah fase perancangan proses sistem informasi maka akan ada dua kemungkinan besar keputusan yaitu apakah akan membeli atau akan membuat. Dalam hal keputusan akan membeli dari vendor tentu maka auditor harus memastikan apakah kemampuan apliaksi yang dibeli akan sanggup melaksnakan fungsi kerja yang sudah ditetapkan sebelumnya, vendornya juga harus diteliti kemampuan dan pengalamannya. Dalam hal pembuatan sendiri sistem maka prosedur dalam desain, koding, kompilasi, testing dan dokumentasi harus dievaluasi dengan seksama oleh auditor. Jadi pada intinya persiapan Request for Proposal (RFP) dan evaluasi proposal akan ditekankan pada tahap ini.

Akuisisi perangkat keras dan lunak – Dalam hal harus membeli suatu harrware atau software baru maka persiapan Request for Proposal (RFP) dan evaluasi proposal akan dilihat. Dalam hal ini auditor harus mencari bukti yang meyakinkan dirinya bahwa proposal itu sudah dipersiapkan dengan baik.

Pengembangan Prosedur - Dalam tahap ini desainer menspesifikasikan aktivitas-aktivitas apa saja yang harus dilakukan oleh user dalam mendukung

jalannya operasi. Dalam hal ini ada beberapa yang harus dipastikan oleh auditor, pertama auditor harus menyakini bahwa kualitas dari prosedur-prosedur tersebut baik. Kedua jika sistem tsb mempunyai dampak yang besar ke segala penjuru perusahan maka sebaiknya tersedia juga prosedur untuk tiap tingkatan level. Ketiga auditor harus mengevaluasi pendekatan yang dilalukan oleh desainer dalam membuat prosedur tesebut. Dan yang terakhir ialah kualiatas dokumentasi harus dipastkan baik.

Uji Penerimaan - Tujuan utama dari uji penerimaan ini ialah untuk mengidentifikasi apakah ada masalah dan penyimpangan yang terjadi dalam proses menuju versi final. Karena alasan kompleksitas maka jarang ada uiji penerimaan yang dilaksanakan secara serentak. Dalam hal ini auditor harus mencari jawaban atas pertanyaan-pertanyaan seperti :

- Bagaimana proses testing dilakukan ?
- Bagaimana test data di rancang dan dikembangkan ?
- Test data apa yang digunakan
- Hasil test apa yang didapatkan ?
- Apa yang dilakukan atas ketidak sesuaian dengan rencana ?
- Apakah semua kendali diuji selama tes tersebut ?

Konversi dan Implementasi - Pada fase konversi ini maka aktivitas-aktivitas yang bertujuan untuk menempatkan sistem yang baru dalam operasi perusahaan dilakukan. Dalam hal ini auditor akan menekankan perhatianya pada (a) kehati-hatian jika terjadi gangguan yang cukup berarti dalam pengujian ini contohnya jika manajemen belum sempat mengidentifikasi masalah dan kebetulan programmer tidak bertanggung jawab memasukkan suatu rutin program untuk kepentingannya pribadi. Hal ini harus dicermati dengan baik. (b) konversi dapat menjadi momen yang tidak bersahabat dan user akan menganggap pendekatan yang dilakukan selama ini tidak baik. Proses pengorganisasian ini sangat diharapkan agar semua berjalan dengan baik.

Operasi dan Pemeliharaan - Perbaikan dan pemeliharaan dan perfective maintenance akan sering terjadi dalam tahap-tahap awal sistem, sedangkan adaptive maintenance akan banyak terjadi di tahap mature sistem. Perhatian utama auditor

dalam hal ini ialah perubahan ini tercatat dengan baik dan pengendalian atas perubahan tersebut tercatat juga.

2. Manajemen Pemrograman

   a. Karakteristik Pemrograman

      Dalam melaksanakan evaluasi atas manajemen pemrograman auditor harus memahami dan memfokuskan perhatiannya pada beberapa karakterisktik program yang berkualitas tinggi, yaitu :

      - Berfungsi secara benar dan lengkap
      - Mempunyai interface pengguna yang berkualitas tinggi
      - Bekerja secara efektif
      - Didesain dan didokumentasikan dengan baik
      - Mudah dipelihara
      - Tahan terhadap kondisi yang abnormal

      Pengendalian atas manajemen pemrograman dapat dilakukan dengan memonitoring tahapan-tahapan yang ditempuh dibandingkan dengan rencana untuk memastikan efisiensi dan ketepatan waktu serta menilai pengendalian yang ada untuk memastikan autentikasi, akurasi dan kelengkapan. Monitoring dapat dilakukan menggunakan work breakdown structure, Gantt charts dan Program Evaluation & Review Techniques (PERT).

      Beberapa hal penting dalam pengendalian manajemen pemrograman antara lain adalah :

      - Gunakan staf pemrograman yang berkualitas tinggi
      - Sedapat mungkin lakukan pemisahan fungsi
      - Kembangkan dan dokumentasikan metodologi dan standar kinerja
      - Batasi kewenangan programer
      - Pelihara log manual dan log komputer atas aktivitas programer
      - Gunakan konsultan luar untuk mengevaluasi pekerjaan pemrograman
      - Lakukan penilaian silang atas kinerja programer secara periodik

b. Evaluasi atas Manajemen Pemrograman

Tahap Perencanaan – Dalam tahap perencanaan yang paling sulit dilakukan adalah perkiraan biaya pemrograman. Auditor sebaiknya mengetahui beberapa teknik perkiraan biaya pemrograman, antara lain :

- Algorithmic Models - Model ini mengestimasikan sumber daya yang diperlukan berdasarkan "cost drivers" nya contohnya estimasi jumlah sumber instruksi yang akan ditulis, bahasa pemrogaraman apa yang akan digunakan, dll. Contoh model ini ialah Boehm's COCOMO model.
- Expert Judgement - Seorang yang ahli dalam hal ini mengestimasi sumber-sumber daya yang diperlukan dalam proyek programming.
- Analogy - Jika proyek yang sama telah pernah dibuat maka sumber daya yang akan diperlukan dapat di estimasi dari sana.
- Top-down Estimation - Pertama proyek dibagi atas tugas- tugas dan sumber daya yang diperlukan di estimasikan berdasarkan proyek-proyek kecil tersebut.
- Bottom-up Estimation - Apabila dari bawah sudah dijelaskan dengan sangat detail apa-apa saja yang harus dikerjakan, maka dari sana bisa dibuat estimasi kebutuhan sumber dayanya dan dengan menyatukan semua itu akan didapatkan estimasi sumber daya keseluruhan pembuatan sistem.

Disamping mengestimasikan sumber daya yang akan digunakan, manajemen juga harus mendiskusikan beberapa pendekatan dibawah ini:

- Pendekatan Desain - Jika program akan dibuat in-house maka manajemen harus menentukan pendekatan apa yang akan dipakai apakah top-down, atau bottom up, atau yang lain.
- Pendekatan Implementasi - Software dapat dibuat in-house, dikontrakkan atau dibeli. Bahasa pemrograman apa yang harus dipilih.
- Pendekatan Integrasi & Testing - Test memerlukan semacam alat pencatat kinerja, dan tanggung jawab integrasi juga perlu dirumuskan pada siapa tanggungjawabnya.

- Organisasi Tim Proyek - Jika sebuah tim ditunjuk untuk mengembangkan atau memutuskan pengadaan software, maka keanggotaan dan struktur timnya harus dijelaskan.

Sebagai auditor dalam fase ini mempunyai dua perhatian yaitu mengevaluasi apakah tingkat dari perencanaan sudah cukup dalam setiap usulan aplikasi yang direncanakan. Hal yang kedua ialah auditor harus memastikan seberapa baikah perencanaan kerja tersebut dilaksanakan.

Tahap Desain - Jika suatu program akan dikembangkan atau dimodiifikasi maka pasti akan ada fase desain. Dalam fase ini programer akan mencari struktur yang jelas tentang apa yang akan dihasilkan oleh sistem ini nantinya. Dalam hal ini akan sangat banyak jenis pendekatan desain model, maka diharapkan seorang auditor mengetahui secara umum dan mengapa programmer umumnya menggunakan pendekatan itu. Contohnya kalau menggunakan third generation langguange seperti COBOL, auditor harus memastikan mengapa menggunakan hal tersebut.

Tahap Coding - Selama tahap coding ini programmer melakukan penulisan program yang pada akhirnya akan membuat program itu menjalankan perintah yang kita inginkan. Sejalan dengan semakin besarnya modul yang akan dibuat maka semakin banyak pula modul-modul di dalamnya. Strategi hubungan antara modul ini ialah :

- Top Down - Dimana dalam strategi ini high level modul di buat dan di integrasikan lebih dahulu sebelum low level modul. Keuntungan pendekatan ini ialah kerusakan pada high level ini yang umumnya sangat serius akan ketahuanduluan, sedangkan keburukannya ialah testing program akan sulit ketika modul low level membuat fungsi input-output (berhubungan ke high level modul).
- Bottom Up - Kebalikan dari atas yatiu duluan low level modul yang dikerjakan dan di integrasikan. Keuntungannya ialah low level modul yang sudah selesai akan dapat digunakan atau dimodifikasi untuk modul lain. Kelemahannya akan sulit mengawasi operasi secara keseluruhan.
- Threads - Dengan pendekatan ini maka fungsi program yang paling penting yang duluan dibuat beserta modul-modulnya. Keuntungannya

ialah fungsi yang paling penting duluan siap. Kelemahannya ialah integrasi dengan modul-modul yang lain akan lebih sulit dari dua pendekatan sebelumnya.

Dalam membuat program maka konvensi umum yang berlaku ialah "GO TO mechanism" yang terbagi secara mendasar menjadi tiga bagian yaitu:

- Simple Sequence (SEQUENCE) - dalam pendekatan ini urutan program akan berurut saja sehabis melakukan A maka program akan menalkukan B, dst.
- Selection Based on a test (IF THEN ELSE) - Dalam pendekatan ini maka program sudah mulai bisa berpikir untuk menggunakan suatu kondisi sebagai pemicu suatu aksi. Jika kondisi A terpenuhi maka akan lakukan C, jika tidak maka lakukan B.
- Conditional Repetition (DO-WHILE) - Dalam pendekatan ini maka setelah suatu langkah akan bisa dianalisa apakah langkah tersebut akan dibuat berulang atau tidak. Selama ia masih memenuhi suatu sayarat ia akan berulang, tetapi jika sudah tidak lagi maka ia akan keluar dari loop tersebut.

Tahap Testing – Tahap ini ditujukan untuk mengidentifikasikan adanya kesalahan, bukan ketidakberadaan kesalahan. Tahap- tahap umum yang ditempuh biasanya adalah (1) Memilih batasan pengujian (2) Menentukan sasaran pengujian (3) Memilih pendekatan pengujian (4) Mengembangkan pengujian (5) Melakukan pengujian (6) Mengevaluasi pengujian dan (7) Mendokumentasikan pengujian

Jenis-jenis Pengujian – Cukup banyak jenis pengujian yang biasanya dilakukan pada tahap ini, antara lain adalah :

- Unit Testing - Memfokuskan evaluasi pada individual modul dalam program, ada dua pendekatan yaitu :

  Analysis test, yaitu mengevaluasi kualiats dari modul melalui pemeriksaan langsung kode sumber. Tes ini terdiri dari : Desk checking, programer memeriksa kode modul untuk mencari kesalahan

seperti melihat logic errors; Strutured walk-through design, programmer yang membuat membantu programmer lain untuk memeriksa modulnya, dari sini akan didapatkan pendapat yang netral dan akan diketahui kesalahan yang ada; Code inspections, Sebuah tim khusus dibentuk untuk melakukan pemeriksaan terhadap modul tersebut.

- Dynamic analytic test, tidak seperti analysis test maka dynamic membutuhkan modul berjalan pada mesin untuk menentukan kesalahannya dimana. Ada dua pendekatan yaitu : black box testing, dalam pendekatan ini maka yang diuji ialah kebutuhan dasar program dan bagaimana keluarannya, jadi program itu sendiri tidak secara langsung di test; white box testing, dalam pendekatan ini maka yang diuji langsung ialah programnya, kode sumbernya, dll.
- Integration Testing - Test ini memfokuskan pengujian pada evalausi sejumlah modul program bersama-sama yang tujuannya untuk (1) melihat pengaruhnya terhadap antarmuka, (2) secara umum apakah mereka gagal memenuhi kebutuhan yang ditetapkan kepada mereka.Tes ini dapat dilakukan dengan cara Big-bang testing, seluruh modul yang di coding secara individual di test secara individu lalu digabung untuk dilihat interaksi antar modul, atau dengan cara Incremental testing, sebagian modul yang mempunyai kemiripan fungsi di test bersamaan kemudian akan digabung dengan modul-modul lain untuk dilihat pengaruh test nya.
- Whole-of-program testing – Tes ini memfokuskan test pada seluruh program secara total, ada empat (4) pendekatan yaitu : Function test, digunakan untuk menjelaskan apakah fungsi- fungsi dari program berjalan dengan baik; Performance test, untuk melihat apakah suatu fungsi tertentu mencapai standar performa tertentu; Acceptance test, untuk melihat apakah semua ketentuan yang ditetapkan sebelumnya dipatuhi oleh program tersebut dalam membuat outputnya;

Installation test, Setelah semua test diatas dilakukan maka selanjutnya dilakukan pengujian install.

Peranan auditor disini adalah untuk melihat apakah semua hal itu berjalan dengan baik atau tidak. Kalau tidak tindakan apa yang dilakukan untuk mengatasinya.

Tahap Operasi & Pemeliharaan – Beberapa aktifitas utama pada tahap ini yang perlu dievaluasi oleh auditor adalah monitoring kinerja dan jenis-jenis pemeliharaan dan perbaikan yang dilakukan serta pengendalian perangkat lunak manajemen konfigurasi yang digunakan.

Nama : **Erwin Satriyansah**
Nim : **182420110**
Kelas : **MTI. 20A**
DosenPengasuh : **Dr Widya Cholil , S.Kom., M.I.T.**
Mata Kuliah : **IT Audit**

Soal

untuk proses control (pengendalian) ada tindakan yang perlu dilaksanakan, gunaka referensi yang ada untuk menjawap pertanyaan saya tertutama dalam hal pengembangan sistem, pemrogramaan dan operasional.

Jawaban

Pengendalian umum atau pengendalian manajemen adalah mengevaluasi aspek-aspek pengendalian umum pada TI apakah sudah dilakukan dengan baik oleh manajemen atau belum.

1. Pengembangan Sistem

Suatu hal yang menjadi perdebatan sejak dahulu ialah mengenai hal yang berfokus pada apakah seorang auditor sebaiknya terlibat dalam tim pengembangan selama proses pengembangan sistem.

a. Pendekatan audit pengembangan sistem

   Auditor dapat memilih salah satu atau kombinasi dari tiga pendekatan berikut ini:

   - Concurrent Audit , Auditor merupakan bagian dari tim pengembangan sistem. Tugas mereka ialah membantu tim pengembangan meningkatkan kualitas sistem pengembanganny.
   - Post implementation Audit, auditor melakukan audit setelah tahap pengembangan sistem selesai dilakukan. Tujuannya ialah guna mengevaluasi sistem yang nantinya akan dihentikan, dilanjutkan ataupun dimodifikasi,
   - General Audit, Auditor menilai pengendalian atas pengembangan sistem secara keseluruhan. Auditor melakukan pendekatanini dengan tujuan untuk dapat mengurangi banyaknya substantive test yang dilakukan untuk menyatakan pendapat.

b. Evaluasi atas pengembangan sistem

   - Defenisi permasalahan, untuk memastikan apakah perusahaan *(stakeholders)* mengetahui apa resiko dan peluang yang mungkin terjadi terkait dengan penambahan suatu sistem informasi tersebut.

- Manajemen perubahan, dengan menitikberatkan pada mempersiapkan perubahan dalam perusahaan dengan pendekatan mendidik *unfreezing the organization)*; berubah ke sistem yang baru *(moving the organization)*; menolong siapa saja yang berkaiatan dengan sistem utnutk beradaptasi dan merasa nyaman dengan sistem yang baru ini *(refreezing the organization)*
- Studi kelayakan

Perlu dilakukan untuk memperoleh komitmen perubahan dari seluruh bagian yang bakal berubah dan mempelajarai secara *cost-effective* apakah perubahan ini bisa dilakukan atau tidak, dan memastkan tidak akan menimbulkan permasalahan dikemudian hari. Ada 4 studi kelayakan yang erlu dilakukan perusahaan yaitu : technical feasibiity, operational feasibility, economic feasibilty, behavioral feasibility.

- Analisa sistem yang ada

Jika sistem yang baru akan direkomendasikan untuk menggantikan sistem yang ada maka ada bebeapa hal yang perlu dilakukan perusahaan yaitu : mempelajari latar belakang, struktur dan budaya organisasi yang ada sekarang untuk mendapatkan pemahaman yang matang; mempelajari arus produk dan informasi yang akan diusulkan sis sietem yang baru.

- Menyusun kebutuhan strategis
- Mendesain organisasi dan pekerjaan
- Mendesain sistem pemrosesan informasi, dengan memeriksa enam aktifitas utama, yaitu :

1. Pendeskripsian kebutuhan strategis untuk meminimalisir ketidakpastian di sekeliling sistem
2. Memastikan bahwa hasil sistem ini memang benar-benar seperti yang diharapkan dan sesuai rencana
3. Mengevaluasi keputusan dalam ruang lingkup database untuk mendefenisikan hal tersebut akan dilaksanakan atau tidak
4. Memastikan pakah desainer sudah mengikuti suatu standar yang berhubungan dengan bagaimana membuat suatu desain yang baik
5. Menitikberatkan perhatian apakah gambaran fisik desain sudah cukup baik atau tidak
6. Memastikan agar desain yang dibuat bisa terintegrasi dengan baik dengan *hardware* atau *software* yang sudah ada.

- Akuisisi/Pengembangan aplikasi
- Akuisisi perangkat lunak
- Pengembangan prosedur
- Uji penerimaan
- Konversi dan implementasi
- Operasi dan pemeliharaan

2. Pemrograman

1. Karakteristik Pemrograman

Dalam melaksanakan evaluasi atas manajemen pemrograman auditor harus memahami dan memfokuskan perhatiannya pada beberapa karakteristik program yang berkualitas tinggi, yaitu :

- Berfungsi secara benar dan lengkap
- Mempunyai interface pengguna yang berkualitas tinggi
- Bekerja secara efektif
- Didesain dan didokumentasikan dengan baik
- Mudah dipelihara
- Tahan terhadap kondisi yang abnormal

Beberapa hal penting dalam pengendalian manajemen pemrograman adalah:

- Gunakan staf pemrograman yang berkualitas tinggi
- Sedapat mungkin lakukan pemisahan fungsi
- Kembangkan dan dokumentasikan metodologi dan standar kinerja
- Batasi kewenangan programer
- Pelihara log manual dan log komputer atas aktivitas program
- Gunakan konsultan luar untuk mengevaluasi pekerjaan pemrograman
- Lakukan penilaian silang atas kinerja programer secara periodik

2. Evaluasi atas manajemen pemrograman

- Tahap perencanaan, Dalam tahap perencanaan yang paling sulit dilakukan adalah perkiraan biaya pemrograman. Audit sebaiknya mengetahui beberapa teknik perkiraan biaya pemrograman.
- Tahap Desain, Jika suatu program akan dikembangkan atau dimodifikasi maka pasti akan ada fase desain. Dalam hal ini akan sangat banyak jenis pendekatan desain model, maka diharapkan seorang auditor mengetahui secara umum dan mengapa programmer umumnya menggunakan pendekatan itu.
- Tahap Coding, Selama tahap coding ini programmer melakukan penulisan progam yang pada akhirnya akan membuat program itu menjalankan perintah yang kita inginkan. Sejalan dengan semakin besarnya modul yang akan dibuat maka semakin banyak pula modul-modul di dalamnya.

- Tahap Testing, Tahap ini di tunjukkan untuk mengidentifikasikan adanya kesalahan, bukan ketidakberadaan kesalahan. Tahap-tahap umum yaitu : memilih batasan pengujian, menentukan sasaran pengujian, memilih pendekatan pengujian, mengembangkan pengujian, melakukan pengujian, mengevaluasi pengujian dan mendokumentasikan pengujian.
- Tahap operasi dan pemeliharaan, Beberapa aktifitas utama pada tahap ini yang perlu dievaluasi oleh auditor adalah monitoring kinerja dan jeni-jenis pemeliharaan dan perbaikan yang dilakukan serta pengendalian perangkat lunak manajemen konfigurasi yang digunakan.

3. Operasional

- Computer Operational Control. Terdiri dari : **operation control** (untuk menentukan apakah fungsi manusia atau operasi otomasi yang harus dilakukan); **schedulling control** (untuk memastikan ahwa sumber daya hardware yang dimiliki oleh perusahaan digunakan hanya oleh personil yang berhak dan hanya digunakan untuk kepentingan perusahaan saja; **maintenance control** (menentukan bagaimana perangkat keras harus dipelihara untuk mencegah kerusakan dan memfungsikan kembali hardware yang rusak.
- Network Operation Control. Terdiri dari LAN controls dan WAN Controls. LAN controls berhubungan dengan kegiatan di Local Area Network, dimana manajemen operasi dalam LAN terjadi melalui fasilitas-fasilitas yang diberikan oleh file server. Wan controls merupakan pengendalian jaringan dalam lingkungan yang lebih luas. Ada suatu keadaan dimana operator harus mengidentifkasi kejadian tertentu dan mengkonfigurasi ulang jaringan untuk mengatasi masalah. Alat yang biasanya berguna untuk jaringan bersar ini disebut Network Control Terminal (NCT) dimana hanya hanya operator senior yang terlatih baik yang akan melaksanakan pengendalian guna menjaga keamanan aset dan integritas data dalam NCT.
- Data Preparation dan Entry

Meliputi :

1. Source document design, dimana sebuah sumber dokumen terstruktur dengan baik, data apa saja yang dicatat, siapa yang mencatat, atau bagaimana dokumen tersebut disimpan ke dalam sistem.
2. Source document storage, dimana sumber yang telah dientry diberi tanda dan tidak boleh dientry kembali dan dikendalikan dengan baik penyimpananya

3. Inpput screen design, dimana perancangan tampilan layr input disesuaikan dengan dokumen sumber dan meperhatikan kemudahan pengguna dan kecepatan entry data.
4. Data entry area design, dimana desain area pemsukan data harus embuat nyaman operator.

- Production control. Meliputi receipt & dispatch of input &output, job schedulling, user service level agreement, transfer pricing or charge out control dan computer consumables.
- File library control. Bertanggung jawab terhadap pengorganisasian penggunaan media penyimpanan, seperti storage of storage media, use of storage media, maintenance and disposal of storage media, location of storage media.
- Documentation and program library control. Auditor dapat mengevalusi dengan menanyakan pada *documentation librarians* tetang tugas mereka, bagaiaman mereka mengorganisir penyimpanan dokumentasi danmemeriksa serta memastikan pencatatan dokumentasi berada dalam tempat yang aman sehingga orang yang tidak bertanggung jawab tidak bisa merubah dan memanfaatkan dokumentasi tersebut.
- Helpdesk/technical support control. Yang berfungsi : membantu end-user menggunakan hardware dan software, menyediakan dukungan y=teknis bagi sistem produksi dengan membantu memecahkan permasalahan.
- Mengevaluasi profil kinerja akan adanya aktifitas yang tidak terotorisasi. Auditor mengevaluasi bagaimana manajemen operasi menorganisir perencanaan kapasitas dan fungsi monitor performance. Akan lebih baik jika tersedia catatan statistik mengenai monitor pekerjaan mereka.
- Management of outsourced operations controls.

Ada 4 pengendalian jika suatu perusahaan akan melakukan outsourcing, yaitu :

1. Evaluasi atas kemampuan finansial vendor
2. Memastikan ketaatan terhadap termin dan kondisi kontrak
3. Memastikan kemampuan untuk mengendalikan operasi vendor
4. Menjaga disaster recovery planning

FAJAR PRAYOGA
182420136
MTI. 20A
IT AUDIT
Oleh Dr Widya Cholil , S.Kom., M.I.T.

Soal

untuk proses control (pengendalian) ada tindakan yang perlu dilaksanakan, gunaka referensi yang ada untuk menjawap pertanyaan saya tertutama dalam hal pengembangan sistem, pemrogramaan dan operasional.

Jawaban

Pengendalian umum atau pengendalian manajemen adalah mengevaluasi aspek-aspek pengendalian umum pada TI apakah sudah dilakukan dengan baik oleh manajemen atau belum.

1. Pengembangan Sistem

Suatu hal yang menjadi perdebatan sejak dahulu ialah mengenai hal yang berfokus pada apakah seorang auditor sebaiknya terlibat dalam tim pengembangan selama proses pengembangan sistem.

a. Pendekatan audit pengembangan sistem

   Auditor dapat memilih salah satu atau kombinasi dari tiga pendekatan berikut ini:

   - Concurrent Audit , Auditor merupakan bagian dari tim pengembangan sistem. Tugas mereka ialah membantu tim pengembangan meningkatkan kualitas sistem pengembanganny.
   - Post implementation Audit, auditor melakukan audit setelah tahap pengembangan sistem selesai dilakukan. Tujuannya ialah guna mengevaluasi sistem yang nantinya akan dihentikan, dilanjutkan ataupun dimodifikasi,
   - General Audit, Auditor menilai pengendalian atas pengembangan sistem secara keseluruhan. Auditor melakukan pendekatanini dengan tujuan untuk dapat mengurangi banyaknya substantive test yang dilakukan untuk menyatakan pendapat.

b. Evaluasi atas pengembangan sistem

   - Defenisi permasalahan, untuk memastikan apakah perusahaan *(stakeholders)* mengetahui apa resiko dan peluang yang mungkin terjadi terkait dengan penambahan suatu sistem informasi tersebut.
   - Manajemen perubahan, dengan menitikberatkan pada mempersiapkan perubahan dalam perusahaan dengan pendekatan mendidik *unfreezing the organization)*; berubah ke sistem yang baru *(moving the organization)*; menolong siapa saja yang

FAJAR PRAYOGA
182420136
MTI. 20A
IT AUDIT
Oleh Dr Widya Cholil , S.Kom., M.I.T.

berkaiatan dengan sistem utnutk beradaptasi dan merasa nyaman dengan sistem yang baru ini *(refreezing the organization)*

- Studi kelayakan

Perlu dilakukan untuk memperoleh komitmen perubahan dari seluruh bagian yang bakal berubah dan mempelajarai secara *cost-effective* apakah perubahan ini bisa dilakukan atau tidak, dan memastkan tidak akan menimbulkan permasalahan dikemudian hari. Ada 4 studi kelayakan yang erlu dilakukan perusahaan yaitu : technical feasibiity, operational feasibility, economic feasibilty, behavioral feasibility.

- Analisa sistem yang ada

Jika sistem yang baru akan direkomendasikan untuk menggantikan sistem yang ada maka ada bebeapa hal yang perlu dilakukan perusahaan yaitu : mempelajari latar belakang, struktur dan budaya organisasi yang ada sekarang untuk mendapatkan pemahaman yang matang; mempelajari arus produk dan informasi yang akan diusulkan sis sietem yang baru.

- Menyusun kebutuhan strategis
- Mendesain organisasi dan pekerjaan
- Mendesain sistem pemrosesan informasi, dengan memeriksa enam aktifitas utama, yaitu :

1. Pendeskripsian kebutuhan strategis untuk meminimalisir ketidakpastian di sekeliling sistem
2. Memastikan bahwa hasil sistem ini memang benar-benar seperti yang diharapkan dan sesuai rencana
3. Mengevaluasi keputusan dalam ruang lingkup database untuk mendefenisikan hal tersebut akan dilaksanakan atau tidak
4. Memastikan pakah desainer sudah mengikuti suatu standar yang berhubungan dengan bagaimana membuat suatu desain yang baik
5. Menitikberatkan perhatian apakah gambaran fisik desain sudah cukup baik atau tidak
6. Memastikan agar desain yang dibuat bisa terintegrasi dengan baik dengan *hardware* atau *software* yang sudah ada.

- Akuisisi/Pengembangan aplikasi
- Akuisisi perangkat lunak
- Pengembangan prosedur
- Uji penerimaan
- Konversi dan implementasi
- Operasi dan pemeliharaan

FAJAR PRAYOGA
182420136
MTI. 20A
IT AUDIT
Oleh Dr Widya Cholil , S.Kom., M.I.T.

2. Pemrograman

1. Karakteristik Pemrograman

Dalam melaksanakan evaluasi atas manajemen pemrograman auditor harus memahami dan memfokuskan perhatiannya pada beberapa karakteristik program yang berkualitas tinggi, yaitu :

- Berfungsi secara benar dan lengkap
- Mempunyai interface pengguna yang berkualitas tinggi
- Bekerja secara efektif
- Didesain dan didokumentasikan dengan baik
- Mudah dipelihara
- Tahan terhadap kondisi yang abnormal

Beberapa hal penting dalam pengendalian manajemen pemrograman adalah:

- Gunakan staf pemrograman yang berkualitas tinggi
- Sedapat mungkin lakukan pemisahan fungsi
- Kembangkan dan dokumentasikan metodologi dan standar kinerja
- Batasi kewenangan programer
- Pelihara log manual dan log komputer atas aktivitas program
- Gunakan konsultan luar untuk mengevaluasi pekerjaan pemrograman
- Lakukan penilaian silang atas kinerja programer secara periodik

2. Evaluasi atas manajemen pemrograman

- Tahap perencanaan, Dalam tahap perencanaan yang paling sulit dilakukan adalah perkiraan biaya pemrograman. Audit sebaiknya mengetahui beberapa teknik perkiraan biaya pemrograman.
- Tahap Desain, Jika suatu program akan dikembangkan atau dimodifikasi maka pasti akan ada fase desain. Dalam hal ini akan sangat banyak jenis pendekatan desain model, maka diharapkan seorang auditor mengetahui

secara umum dan mengapa programmer umumnya menggunakan pendekatan itu.

- Tahap Coding, Selama tahap coding ini programmer melakukan penulisan progam yang pada akhirnya akan membuat program itu menjalankan perintah yang kita inginkan. Sejalan dengan semakin besarnya modul yang akan dibuat maka semakin banyak pula modul-modul di dalamnya.
- Tahap Testing, Tahap ini di tunjukkan untuk mengidentifikasikan adanya kesalahan, bukan ketidakberadaan kesalahan. Tahap-tahap umum yaitu : memilih batasan pengujian, menentukan sasaran pengujian, memilih pendekatan pengujian, mengembangkan pengujian, melakukan pengujian, mengevaluasi pengujian dan mendokumentasikan pengujian.
- Tahap operasi dan pemeliharaan, Beberapa aktifitas utama pada tahap ini yang perlu dievaluasi oleh auditor adalah monitoring kinerja dan jenis-jenis pemeliharaan dan perbaikan yang dilakukan serta pengendalian perangkat lunak manajemen konfigurasi yang digunakan.

3. Operasional

- Computer Operational Control. Terdiri dari : **operation control** (untuk menentukan apakah fungsi manusia atau operasi otomasi yang harus dilakukan); **schedulling control** (untuk memastikan ahwa sumber daya hardware yang dimiliki oleh perusahaan digunakan hanya oleh personil yang berhak dan hanya digunakan untuk kepentingan perusahaan saja; **maintenance control** (menentukan bagaimana perangkat keras harus dipelihara untuk mencegah kerusakan dan memfungsikan kembali hardware yang rusak.
- Network Operation Control. Terdiri dari LAN controls dan WAN Controls. LAN controls berhubungan dengan kegiatan di Local Area Network, dimana manajemen operasi dalam LAN terjadi melalui fasilitas-fasilitas yang diberikan oleh file server. Wan controls merupakan pengendalian jaringan dalam lingkungan yang lebih luas. Ada suatu keadaan dimana operator harus mengidentifkasi kejadian tertentu dan mengkonfigurasi ulang jaringan untuk mengatasi masalah. Alat yang biasanya berguna untuk jaringan bersar ini disebut Network Control Terminal (NCT) dimana

FAJAR PRAYOGA
182420136
MTI. 20A
IT AUDIT
Oleh Dr Widya Cholil , S.Kom., M.I.T.

hanya hanya operator senior yang terlatih baik yang akan melaksanakan pengendalian guna menjaga keamanan aset dan integritas data dalam NCT.

- Data Preparation dan Entry

Meliputi :

1. Source document design, dimana sebuah sumber dokumen terstruktur dengan baik, data apa saja yang dicatat, siapa yang mencatat, atau bagaimana dokumen tersebut disimpan ke dalam sistem.
2. Source document storage, dimana sumber yang telah dientry diberi tanda dan tidak boleh dientry kembali dan dikendalikan dengan baik penyimpananya
3. Inpput screen design, dimana perancangan tampilan layr input disesuaikan dengan dokumen sumber dan meperhatikan kemudahan pengguna dan kecepatan entry data.
4. Data entry area design, dimana desain area pemsukan data harus embuat nyaman operator.

- Production control. Meliputi receipt & dispatch of input &output, job schedulling, user service level agreement, transfer pricing or charge out control dan computer consumables.
- File library control. Bertanggung jawab terhadap pengorganisasian penggunaan media penyimpanan, seperti storage of storage media, use of storage media, maintenance and disposal of storage media, location of storage media.
- Documentation and program library control. Auditor dapat mengevalusi dengan menanyakan pada *documentation librarians* tetang tugas mereka, bagaiaman mereka mengorganisir penyimpanan dokumentasi danmemeriksa serta memastikan pencatatan dokumentasi berada dalam tempat yang aman sehingga orang yang tidak bertanggung jawab tidak bisa merubah dan memanfaatkan dokumentasi tersebut.
- Helpdesk/technical support control. Yang berfungsi : membantu end-user menggunakan hardware dan software, menyediakan dukungan y=teknis bagi sistem produksi dengan membantu memecahkan permasalahan.
- Mengevaluasi profil kinerja akan adanya aktifitas yang tidak terotorisasi. Auditor mengevaluasi bagaimana manajemen operasi menorganisir perencanaan kapasitas dan fungsi monitor performance. Akan lebih baik jika tersedia catatan statistik mengenai monitor pekerjaan mereka.
- Management of outsourced operations controls.

Ada 4 pengendalian jika suatu perusahaan akan melakukan outsourcing, yaitu :

1. Evaluasi atas kemampuan finansial vendor
2. Memastikan ketaatan terhadap termin dan kondisi kontrak
3. Memastikan kemampuan untuk mengendalikan operasi vendor
4. Menjaga disaster recovery planning

NAMA (NIM) : **Gian Pratama (182420116)**

KELAS : **MTI 20A**

TUGAS : **Control & Audit IT**

TINDAKAN YANG PERLU DILAKUKAN DALAM PROSES CONTROL (PENGENDALIAN) AUDIT IT

1. Pengendalian Umum

Pengendalian umum pada perusahaan dilakukan terhadap aspek fisikal maupun logikal. Aspek fisikal dilakukan terhadap aset-aset fisik perusahaan, sedangkan aspek logikal terhadap sistem informasi di level manajemen (misal: sistem operasi). Pengendalian umum sendiri digolongkan menjadi beberapa, diantaranya:

a. Pengendalian organisasi dan otorisasi. Yang dimaksud dengan pengendalian organisasi adalah secara umum terdapat pemisahan tugas dan jabatan antara pengguna sistem (operasi) dan administrator sistem (operasi). Dan juga dapat dilihat bahwa pengguna hanya dapat mengakses sistem apabila memang telah diotorisasi oleh *administrator*.

b. Pengendalian operasi. Operasi sistem informasi dalam perusahaan juga perlu pengendalian untuk memastikan sistem informasi tersebut dapat beroperasi dengan baik selayaknya sesuai yang diharapkan.

c. Pengendalian perubahan. Perubahan-perubahan yang dilakukan terhadap sistem informasi harus dikendalikan, termasuk pengendalian versi dari sistem informasi tersebut, catatan perubahan versi, serta manajemen perubahan atas diimplementasikannya sebuah sistem informasi.

d. Pengendalian akses fisikal dan logikal. Pengendalian akses fisikal berkaitan dengan akses secara fisik terhadap fasilitas-fasilitas sistem informasi suatu perusahaan, sedangkan akses logikal berkaitan dengan pengelolaan akses terhadap sistem operasi sistem tersebut (misal: Windows).

2. Pengendalian Aplikasi

Pengendalian aplikasi (*application controls*) adalah sistem pengendalian intern (*internal control*) pada sistem informasi berbasis teknologi informasi yang berkaitan dengan pekerjaan, kegiatan atau aplikasi tertentu (setiap aplikasi memiliki karakteristik dan kebutuhan pengendalian yang berbeda). Tujuan pengendalian aplikasi dimaksudkan untuk memastikan bahwa data di-input secara benar ke dalam aplikasi, diproses secara benar, dan terdapat pengendalian yang memadai atas *output* yang dihasilkan. Dalam audit terhadap aplikasi, biasanya, pemeriksaan atas pengendalian umum juga dilakukan mengingat pengendalian umum memiliki kontribusi terhadap efektifitas atas pengendalian-pengendalian aplikasi.

2.1. Pengendalian batas sistem (*boundary controls*)

Adalah interface antara users dengan sistem berbasis teknologi informasi. Tujuan utama boundary controls antara lain :

a) Untuk mengenal identitas dan otentik / tidaknya pemakai sistem.

b) Untuk menjaga agar sumber daya sistem informasi digunakan oleh user dengan cara yang ditetapkan.

2.2. Pengendalian masukan (*input controls*)

Bertujuan untuk mendapat keyakinan bahwa data transaksi input adalah valid, lengkap, serta bebas dari kesalahan dan penyalahgunaan. *Input controls* merupakan pengendalian aplikasi yang penting karena input yang salah akan menyebabkan *output* yang salah.

2.3. Pengendalian proses pengolahan data (*process controls*)

Pengendalian proses (processing controls) ialah pengendalian intern untuk mendeteksi jangan sampai data (khususnya data yang sesungguhnya sudah valid) menjadi error karena adanya kesalahan proses.

Kemungkinan yang paling besar untuk menimbulkan terjadinya error adalah kesalahan logika program, salah rumus, salah urutan program, ketidakterpaduan antar subsistem atupun kesalahan teknis lainnya.

2.4. Pengendalian keluaran (*output controls*)

Merupakan pengendalian yang dilakukan untuk menjaga output sistem agar akurat, lengkap, dan digunakan sebagaimana mestinya. Yang termasuk pengendalian keluaran antara lain adalah :

a) Rekonsiliasi keluaran dengan masukan dan pengolahan

b) Penelaahan dan pengujian hasil – hasil pengolahan

2.4. Pengendalian file / database (*file/database controls*)

Merupakan pengendalian yang dilakukan untuk menjaga sistem database yang berperan mendefinisikan, membuat, memodifikasi, menghapus, dan membaca data dalam sistem informasi dapat digunakan sebagaimana mestinya ketika dibutuhkan. Komponen utama dalam subsistem database antara lain: *database management system, application programs, central processor & primary storage,* dan *storage media.*

Referensi :

Whida Nadya Cantika. Pengendalian Audit Sistem Informasi. Universitas Mitra Indonesia.

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=7&ved=2ahUKEwj95obkvpzpAhVMb30KHYstCgcQFjAGegQIBhAB&url=https%3A%2F%2Fosf.io%2Fngqxh%2Fdownload&usg=AOvVaw1-TTXuaYWlxH3bBIIHfpTV

Contol & Audit TI

Universitas Bina Darma

Tindakan yang perlu dilaksanakan dalam proses control (pengendalian)

1. Control Pengembangan Sistem
2. Control Pemograman
3. Control Operasional

Hari Febriadi (182420127)

MTI.20A

Contol & Audit TI

Universitas Bina Darma

Tindakan pada pengembangan sistem

Manajemen pengembangan sistem bertanggung jawab terhadap proses penganalisaan, Perancangan, pembangunan, penerapan, pemeliharaan sistem informasi.

pada fase ini menguraikan bagaimana kita dapat melakukan audir subsistem manajemen pengembangan sistem dengan mempertimbangkan 3 cara pendekatan audit sebagai pelaku di dalam proses pengembangan sistem.

Hari Febriadi (18242012?)

MTI.20A

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Contol & Audit TI

Universitas Bina Darma

Tindakan pada pengembangan sistem

3 Cara Pendekatan AUDIT

1. **CONCURENT AUDIT** : Auditor sebagai anggota tim pengembangan sistem.

2. **POSTIMPLEMENTION AUDIT** : Auditor mencari untuk membantu organisasi belajar dari pengalaman dalam pengembangan sistem aplikasi yang spesifik.

Hari Febriadi (18242012?)

MTI.20A

IT AUDIT : Control and Audit TI

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Contol & Audit TI

Universitas Bina Darma

Tindakan pada pengembangan sistem

3. **GENERAL AUDIT** : Auditor mengevaluasi pengendalian pengembangan sistem secara menyeluruh.

3 Cara Pendekatan AUDIT

Hari Febriadi (182420127)

MTI.20A

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Contol & Audit TI

Universitas Bina Darma

Tindakan pada Pemograman

Pada fase ini lebih mengarah kepada praktek-praktek yang mengarah pada produksi / akuisisi perangkat lunak kualitas tinggi.

Tujuan dari fase ini adalah untuk menghasilkan atau melaksanakan dan memperoleh program-program berkualitas tinggi.

Hari Febriadi (182420127)

MTI.20A

IT AUDIT : Control and Audit TI

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Contol & Audit TI

Universitas Bina Darma

Tindakan pada Operasional

Pada fase ini lebih mengarah kepada proses meyakinkan bahwa tiap-tiap tugas telah dilaksanakan secara efektif dan efisien.

Dapat disimpulkan bahwa kegiatan-kegiatan dalam manajemen tingkat atas lebih menjurus ke perencanaan jangka panjang dan penentuan-penentuan strategi. lebih bawah tingkatannya, kegiatan manajemen lebih menjurus ke hal-hal yang sifatnya operasional.

Hari Febriadi (182420127)

MTI.20A

IT AUDIT : Control and Audit TI

Dosen Pembimbing : Dr Widya Cholil , S.Kom., M.I.T.

Nama : Harli Septia Fani
NIM : 182420122
Kelas : MTI 20A
Mata Kuliah : IT Audit
Dosen : Dr. Widya Cholil, S. Kom., M. IT.

Soal :

untuk proses control (pengendalian) ada tindakan yang perlu dilaksanakan, gunaka referensi yang ada untuk menjawap pertanyaan saya tertutama dalam hal pengembangan sistem, pemrogramaan dan operasional

Pembahasan :

PENGENDALIAN MANAJEMEN

1. Pengembangan Sistem
   a) Melakukan pendekatan audit.
      Ada beberapa pendekatan audit yang bisa dipilih auditor :
      - ✓ Membantu tim pengembangan meningkatkan kualitas sistem pengembangannya (Concurrent Audit)
      - ✓ Mengevaluasi sistem setelah selesai tahap proses pengembangan untuk menentukan apakah sisten tersebut apakah akan dihentikan, dilanjutkan atau dimodifikasi (Post Implementation Audit)
      - ✓ Menilai pengembangan sistem secara keseluruhan untuk mengurangi banyaknya *substantive test* yang dilakukan dalam menyatakan pendapat (General Audit)
   b) Melakukan evaluasi Pengembangan Sistem
      - ✓ Defenisi permasalahan, untuk memastikan apakah perusahaan *(stakeholders)* mengetahui apa resiko dan peluang yang mungkin terjadi terkait dengan penambahan suatu sistem informasi tersebut.
      - ✓ Manajemen perubahan, dengan menitikberatkan pada mempersiapkan perubahan dalam perusahaan dengan pendekatan mendidik *unfreezing the organization)*; berubah ke sistem yang baru *(moving the organization)*; menolong siapa saja yang berkaiatan dengan sistem utnutk beradaptasi dan merasa nyaman dengan sistem yang baru ini *(refreezing the organization)*
      - ✓ Studi kelayakan

Perlu dilakukan untuk memperoleh komitmen perubahan dari seluruh bagian yang bakal berubah dan mempelajarai secara *cost-effective* apakah perubahan ini bisa dilakukan atau tidak, dan memastkan tidak akan menimbulkan permasalahan dikemudian hari. Ada 4 studi kelayakan yang erlu dilakukan perusahaan yaitu : technical feasibiity, operational feasibility, economic feasibilty, behavioral feasibility.

- ✓ Analisa sistem yang ada
  Jika sistem yang baru akan direkomendasikan untuk menggantikan sistem yang ada maka ada bebeapa hal yang perlu dilakukan perusahaan yaitu : mempelajari latar belakang, struktur dan budaya organisasi yang ada sekarang untuk mendapatkan pemahaman yang matang; mempelajari arus produk dan informasi yang akan diusulkan sis sietem yang baru.
- ✓ Menyusun kebutuhan strategis
- ✓ Mendesain organisasi dan pekerjaan
- ✓ Mendesain sistem pemrosesan informasi, dengan memeriksa enam aktifitas utama, yaitu :
  1. Pendeskripsian kebutuhan strategis untuk meminimalisir ketidakpastian di sekeliling sistem
  2. Memastikan bahwa hasil sistem ini memang benar-benar seperti yang diharapkan dan sesuai rencana
  3. Mengevaluasi keputusan dalam ruang lingkup database untuk mendefenisikan hal tersebut akan dilaksanakan atau tidak
  4. Memastikan pakah desainer sudah mengikuti suatu standar yang berhubungan dengan bagaimana membuat suatu desain yang baik
  5. Menitikberatkan perhatian apakah gambaran fisik desain sudah cukup baik atau tidak
  6. Memastikan agar desain yang dibuat bisa terintegrasi dengan baik dengan *hardware* atau *software* yang sudah ada.
- ✓ Akuisisi/Pengembangan aplikasi
- ✓ Akuisisi perangkat lunak
- ✓ Pengembangan prosedur
- ✓ Uji penerimaan
- ✓ Konversi dan implementasi
- ✓ Operasi dan pemeliharaan

2. Manajemen Pemrograman
   - ✓ Memahami dan fokus pada karakteristik program berkualitas tinggi, pengendalian manajemen pemrograman seperti : gunakan staf pemrograman berkualitas tinggi. Lakukan pemisahan fungsi, batasi kewenangan programer, dan hal penting lainnya.

- ✓ Evaluasi atas manajemen pemrograman
  Terdiri dari beberapa tahap, yaitu :
  1. Perencanaan . Sebagai auditor harus mengevaluasi apakah tingkt perencanaan sudah cukup dalam setiap usulan aplikasi yang direncanakan dan harus memastikan seberapa baikkah perencanaan kerja tersebut dilaksanakan.
  2. Desain. Auditor harus mengetahui alasan dan memastikan mengapa programmer menggunakan psuatu pendekatan desain model tertentu.
  3. Coding. Dimana programmer malekukan penulisan program yang pada akhirnya akan membuat program itu menjalankan perintah yang kita inginkan.
  4. Testing. Ditujukan untuk mengidentifikasikan adanya kesalahan, dengan menggunakan tahapan umum, yaitu : memilih batasan pengujian, menentukan sasaran pengujian, memilih pnedekatan penggujian, mengembangkan pengujian, melakukan pengujian, mengevaluasi pengujian, dan mendokumentasikan pengujian.
  5. Opersi dan pemeliharaan. Auditor memonitoring kinerja dan jenis-jenis pemeliharaan dan perbaikan yang dilakukan serta pengendalian perangat lunak manajemen konfigurasi yang digunakan.

3. Manajemen Operasional
   - ✓ Computer Operational Control. Terdiri dari : **operation control** (untuk menentukan apakah fungsi manusia atau operasi otomasi yang harus dilakukan); **schedulling control** (untuk memastikan ahwa sumber daya hardware yang dimiliki oleh perusahaan digunakan hanya oleh personil yang berhak dan hanya digunakan untuk kepentingan perusahaan saja; **maintenance control** (menentukan bagaimana perangkat keras harus dipelihara untuk mencegah kerusakan dan memfungsikan kembali hardware yang rusak.
   - ✓ Network Operation Control. Terdiri dari LAN controls dan WAN Controls. LAN controls berhubungan dengan kegiatan di Local Area Network, dimana manajemen operasi dalam LAN terjadi melalui fasilitas-fasilitas yang diberikan oleh file server. Wan controls merupakan pengendalian jaringan dalam lingkungan yang lebih luas. Ada suatu keadaan dimana operator harus mengidentifkasi kejadian tertentu dan mengkonfigurasi ulang jaringan untuk mengatasi masalah. Alat yang biasanya berguna untuk jaringan bersar ini disebut Network Control Terminal (NCT) dimana hanya hanya operator senior yang terlatih baik yang akan melaksanakan pengendalian guna menjaga keamanan aset dan integritas data dalam NCT.
   - ✓ Data Preparation dan Entry
     Meliputi :

1. Source document design, dimana sebuah sumber dokumen terstruktur dengan baik, data apa saja yang dicatat, siapa yang mencatat, atau bagaimana dokumen tersebut disimpan ke dalam sistem.
2. Source document storage, dimana sumber yang telah dientry diberi tanda dan tidak boleh dientry kembali dan dikendalikan dengan baik penyimpananya
3. Inpput screen design, dimana perancangan tampilan layr input disesuaikan dengan dokumen sumber dan meperhatikan kemudahan pengguna dan kecepatan entry data.
4. Data entry area design, dimana desain area pemsukan data harus embuat nyaman operator.

- ✓ Production control. Meliputi receipt & dispatch of input &output, job schedulling, user service level agreement, transfer pricing or charge out control dan computer consumables.
- ✓ File library control. Bertanggung jawab terhadap pengorganisasian penggunaan media penyimpanan, seperti storage of storage media, use of storage media, maintenance and disposal of storage media, location of storage media.
- ✓ Documentation and program library control. Auditor dapat mengevalusi dengan menanyakan pada *documentation librarians* tetang tugas mereka, bagaiaman mereka mengorganisir penyimpanan dokumentasi danmemeriksa serta memastikan pencatatan dokumentasi berada dalam tempat yang aman sehingga orang yang tidak bertanggung jawab tidak bisa merubah dan memanfaatkan dokumentasi tersebut.
- ✓ Helpdesk/technical support control. Yang berfungsi : membantu end-user menggunakan hardware dan software, menyediakan dukungan y=teknis bagi sistem produksi dengan membantu memecahkan permasalahan.
- ✓ Mengevaluasi profil kinerja akan adanya aktifitas yang tidak terotorisasi. Auditor mengevaluasi bagaimana manajemen operasi menorganisir perencanaan kapasitas dan fungsi monitor performance. Akan lebih baik jika tersedia catatan statistik mengenai monitor pekerjaan mereka.
- ✓ Management of outsourced operations controls.
  Ada 4 pengendalian jika suatu perusahaan akan melakukan outsourcing, yaitu :
  1. Evaluasi atas kemampuan finansial vendor
  2. Memastikan ketaatan terhadap termin dan kondisi kontrak
  3. Memastikan kemampuan untuk mengendalikan operasi vendor
  4. Menjaga disaster recovery planning

Nama : I Made Harya Wijaya Oka Rafflesia
NIM : 182420129
Matkul : IT Audit
Tanggal : 30 April 2020

SIKLUS PENGEMBANGAN SISTEM INFORMASI

Salah satu kunci IT Gevermence dalam pandangan kontrol internal adalah perlunya kebijakan formal dari tiap manegement mengenai metologi perkembangan sistem (System Development metodology). Pucuk pimpinan perusahaan harus menetapkan metologi system development life cycle seal yang dianut.

Siklus Hidup Sistem

Siklus daur hidup sistem (system life cycle) adalah proses evolusioner yang terjadi dalam penerapan sistem atau sub sistem informasi berbasis komputer. Mulai dari perencanaan kebutuhan sistem sampai dioperasokan untuk kegiatan organisasi. Proses tersebut terdiri dari kegiatan perencanaan, analisis, rancangan (Design / construction), penerapan (System Implementation), dan penggunaan sistem atau sering disebut dengan istilah production (operasionalisasi sistem) sebagai suatu sistem yang life digunakan sesuai kebutuhan pengguna dari pada tahap penggunaan tersebut seluruh operasi sistem dilakukan oleh pengguna.

Sistem informasi dibangun menurut kaidah dan metoda – metoda tertentu yang disebut metodologi (System Depelopment Methodology). Menurut berbagai sumber lain, terdapat metodologi yang dapat diikuti.

Sistem development life cycle (SDLC) adalah seluruh proses mengembangkan produknya membangun sistem informasi melalui berbagai langkah, mulai dari penelitian kebutuhan (requitment), analisis, desain, implementasi dan pemeliharaan (maintenance).

Tahap	Keterangan
Fensibility study	Menentukan layak/tidaknya, cost-beneft satu proses sistem.
Information Analysis	Menggali user requirements.
System Design	Merancang user interface, sistem file, dan information processing functions yang akan dilakukan, dan sebagainya.
Program development	Memdesain, coding, compiling, testing, dan decomenting programs.
Procedures and forms devenlopment	Mendesain system procedures dan form – form yang akan digunakan.
Acceplance testing	Final text / formal approval / accerptanes dari out
Conversion	Implementasi, mengganti sistem lama dengan sistem baru.
Operation and maintenance	On-gving production, eperasionalisasi sistem, perawatan dan perbaikan, evaluasi atau usul sistem yang lebih baru lagi di kemudian hari.

Tabel 9.1 Tahap – tahap Perkembangan System

Secara lebih rinci kegiatan – kegiatan dalam berbagai tahap pengembangan sistem aplikasi tersebut dapat diuraikan sebagai berikut :

1. The Planning Phase

Kegiatan – kegiatan yang dilakukan pada tahap ini antara lain adalah :

· Mengenali masalah yang dihadapi (recognize the prolem)
· Merumuskan problem yang sesungguhnya (define the problem)
· Menetapkan tujuan / sasaran (Set system objectives)
· Identifikasi kendala / keterbatasan (Identify system constraint)
· Melakukan studi kelayakan (conduct a feasibility study); mengamati faktur – faktur yang berpengaruh terhadap pencapaian tujuan, mencakup kelayakan.
· Menyiapkan proposal (Prepare a system study proposal)
· Disetujui / tidaknya usulan (approce or disapprove the study project)
· Membangun mekanisme kontrol (establish a control mechinisme)

2. The analysis Phase

Dalam tahap system analysis dilakukan studi tentang sistem yang berjalan saat ini (existing / eurrent system) dalam rangka menilai ada / tidaknya kelemahan.

· Membentuk tim
· Merumuskan tujuan atau kebutuhan informasi
· Merumuskan system performance cycle
· Menyiapkan design proposal.

3. The implementasi phase

Pada tahap implementasi dilakukan acquisition dan integrasi sumber daya fisik dan no fisik agar sistem dapat dioperasikan.

· Perencanaan implementasi dan mengumumkannya
· Perolehan sumber daya hardware dan software
· Menyiapkan fasilitas fisik
· Pelatihan users
· Menyiapkan the cutever proposal dan cutover the new system

4. The use phase

Antara lain kegiatan – kegiatan sebagai berikut :

· Penggunaan sistem (use the system)
· Evaluasi atau pemeriksaan (Audit the system)

5. Maintain the system

· Melakukan perbaikan, memutakhirkan dan menyempurkan use (to keep system current / to improses the system)
· Menyiapkan usulan renginsering bila diperlukan.

Pemeliharaan / Modifikasi Sistem

Sistem yang sudah operasional seringkali penting untuk disempurnakan di-update, di-generate laporan – laporan tambahan, atau perubahan – perubahan minor. Salah satu alasan untuk melakukan perubahan adalah karena tidaklah mungkin untuk mengatasi seluruh kontinjensi selama tahap perancangan. Selain itu, kondisi lingkungan bisnis membutuhkan perubahan.

Aspek – aspek atau tahap yang mana saja yang diperlu dievaluasi dari satu kegiatan pengembangan sistem aplikasi? Ada beberapa hal yang harus dievaluasi yaitu. (a) Problem opportunity definition, (b) management of the change procces, (c) entry the feasibility assessment, (d) Analysis of the existing system, (e) formulation of strategic requirements, (f) Organizational and job design, (g) Information processing system design, (h) application software acquisition and development, (i) hardware/system software acquisition, (j) procedures development, (k) acceplence testing, (l) conversion, (m) operation and maintenance.

Sumber : http://fitharikhadir.blogspot.com/2016/01/audit-sistem-informasi-dan-prosedur.html

Tindakan yang perlu dilaksanakan Pada Proses Control (Pengendalaian)

Manajemen Pengembangan Sistem

Suatu hal yang menjadi perdepatan sejak dulu ialah mengenai hal yang berfokus pada apakan seorang auditor sebaiknya terlibat dalam tim pengembangan selama proses pengembangan sistem. Bagi yang mendukung hal ini memberikan argumen karena di tahap inilah kesalahan-kesalahan sebaiknya diperbaiki. Sebaliknya bagi yang menolak beragumen tidak sepantasnya siapa yang bakal meng-audit sistem ini nantinya turut serta pula membangun sistem ini karena akan menimbulkan conflict of interest pada saat audit.

1. **Pendekatan Audit Pengembangan Sistem**
   Auditor dapat memilih salah satu atau kombinasi dari tiga pendekatan berikut ini dalam melakukan audit atas pengembangan sistem:
   - **Concurrent Audit** – Auditor merupakan bagian dari tim pengembangan sistem. Tugas mereka ialah membantu tim pengembangan meningkatkan kualaitas sistem pengembangannya.
   - **Post Implementation Audit** – Auditor melakukan audit setelah tahap pengembangan sistem selesai dilakukan. Tujuannya ialah guna mengevaluasi sistem yang nantinya akan dihentikan, dilanjutkan ataupun dimodifikasi.
   - **General Audit** – Auditor menilai pengendalian atas pengembangan sistem secara keseluruhan. Auditor melakukan pendekatan ini dengan tujuan untuk dapat mengurangi banyaknya substantive test yang dilakukan untuk menyatakan pendapat.

2. **Evaluasi Pengembangan Sistem**
   Definsi Permasalahan – Sistem informasi dibuat untuk mengatasi permasalahana ataupun mengambil keuntungan ari peluang yang ada. Auditor mustinya mempunyai empat (4) keingintahuan di benaknya dalam menyikapi hal ini, yaitu:
   - Apakah kemungkinan penyelesaian sistem informasi akan berdampak material dalam hal besar dan berpengaruh terhadap perusahaan?
   - Jika nantinya sistem informasi akan merubah jalannya perusahaan pada tingkatan mana sajakah yang akan berubah?
   - Jika nantinya sistem informasi memiliki ketidakpastian mengenai teknologi yang digunakan, apakah sudah diambil tindakan untuk mengurangi ketidakpastian itu?
   - Apakah seluruh jajaranan perusahaan (stakeholder) setuju pada pendefinisian masalah dan peluang yang ada? Jika tidak tindakan apa yang diambil oleh manajemen untuk mengambil jalah tengahnya?

   Tujuan keingintahuan ini ialah untuk memastikan apakah perusahanaan (stakeholders) mengetahui apa resiko dan peluang yang mungkin terjadi terkait dengan penambahan syatu sistem informasi tersebut.

Manajeman Perubahan – Manajemen perubahan berjalan bersamaan dengan semua proses dalam pengembangan sistem. Ada tiga (3) aktivitas yang perlu dilakukan perusahaan selama perubahan ini yaitu :

- **Unfreezing the organization** – yaitu mempersiapkan perubahan dalam perusahaan dengan pendekatan mendidik.
- **Moving the organization** – yaitu berubah ke sistem yang baru dibuat.
- **Refreezing the organization** – yaitu menolong siapa saja yang berkitan dengan sistem ini untuk beradaptasi dan merasa nyaman dengan sistem yang baru ini.

Selama proses ini auditor menitikberatkan pengamatan pada prose transformasi ini.

Studi Kelayakan – Tujuan dari bagian ini ialah untuk memperoleh komitmen perubahan ini seluruh bagian yang bakal berubah dan mempelajari secara cost-effective apakah perubahan ini masih bisa dilakukan atau tidak. Ada empat (4) studi kelayakan yang perlu dilakukan oleh perusahaan yaitu :

- **Technical Feasibility** – Apakah teknologi yang ada saat ini sanggup menjalankan sistem yang akan dibuat? dapatkah teknologi tersebut dibuat dan diselesaikan?
- **Operational Feasibility** – Apakah data yang di masukkan ke sistem dapat dikumpulkan oleh sistem? Apakah hasil keluarannya dapat berguna?
- **Economic Feasibility** – apakah biaya pembuatan sistem ini nantinya akan lebih kecil dari manfaat yang akan didapatksn dari sistem ini nantinya?
- **Behavioral Feasibility** – Dampak apa sajakah yang akan terjadi pada pengguna?

Analisis Kelayakan yang berjalan - Apabila sistem baru akan di rekomendasikan untuk menggantikan sistem yang ada. Desainer dari sistem perlu mengetahui sistem yang sudah ada. Ada beberapa yang perlu dilakukan oleh perusahaan yaitu:

Menyusun Kebutuhan Strategis – Kebutuhan stragegik yang perlu dipenuhi oleh sistem ialah tujuan dari sistem yang kongkrit. Seperti mengurangi tingkat perputaran staf dalam area penjualan sebesar 30%. Auditor dalam hal ini harus memusatkan perhatiannya pada apakah desainer dari sistem menyadari betul pentingnya kebutuhan strategik ini.

Mendesain Organisasi dan Pekerjaan – Dalam beberapa kasus, untuk mencapai kebutuhan strategis diperlukan desain atau desain ulang dari struktur organisasi dan pekerjaan. Jika auditor sudah dapat memastikan bahwa langkah ini bukan merupakan masalah lagi, ini berarati auditor dapat mengurangi tingkat resiko pengendalian yang berkaitan dengan pengembangan sistem. Jika tidak maka auditor harus meninjau ulang pendapat mereka tentang resiko pengendalian di bidang ini dan berencana meningkatkan substantive test.

Mendesain Sistem Pemrosesan informasi – Ketika mengevaluasi fase desain sistem pemrosesan informasi, baik itu sebagai partisipan dalam proses desain ataupun audit setelah implementasi, seorang auditor harus memeriksa enam aktiviatas utama yaitu :

- Elicitation of Detailed Requirement
- Design of Data/Information Flow
- Design of Database

- Design of User Interface
- Physical Design
- Design & Acquisition of Hardware Platfrom
- Akuisisi Pengembangan Aplikasi
- Akusisi Perangkat Keras dan Lunak
- Pembanganan Prosedur
- Uji Penerimaan
- Konversi dan Implementasi
- Operasi dan Pemeliharaan

Manajemen Pemprograman

Karakateristik Pemprograman

Dalam melaksanakan evaluasi atas manajemen pemrogman auditor harus memahami dan memfokuskan perhatiannya pada beberapa karakteristik program yang berkualitas tinggi, yaitu:

- Berfungsi secara benar dan lenyap
- Mempunyai interface pengguna yang berkualitas tinggi
- Bekerja secara efektif
- Desain dan didokumentasikan dengan baik
- Mudah dipelihara
- Tahap terhadap kondisi yang abnormal

Evaluasi Managemen Pemrograman

Tahap Perencanaan – Dalam tahap perencanaan yang paling sulit dilakukan adalah perkiraan biaya pemrograman. Auditor sebaiknya mengetahui beberapa teknik perkiraan biaya pemrograman, antara lain :

- **Algorithmic Models**
- **Expert Judgement**
- **Analogy**
- **Top Down Estimation**
- **Bottom Up Estimation**

Disamping mengestimasi sumber daya yang akan digunakan, manajemen juga harus mendiskusikan beberapa pendekatan dibawah ini :

- **Pendekatan Desain**
- **Pendekatan Implementasi**
- **Pendekatan Integrasi & Testing**
- **Organisasi Tim Proyek**

Tahap Desain – Jika suatu program akan dikembangkan atau dimodivikasi maka pasti akan ada fase desain. Falam fase ini programer akan mencari struktur yang jelas tentang apa yang akan dihasilkan oleh sistem ini nantinya. Dalam hal ini akan sangat banyak jenis pendekatan desain model, maka diharapkan seoran auditor mengetahui secara umum dan mengapa programmer umumnya third generation langguage seperti COBOL, auditor harus memastikan mengapa mengunakan hal tersebut.

Tahap Coding – Selama tahap coding ini programmer melakukan penulisan program yang pada akhirnya akan membuat program itu menjalankan yang kita inikan. Sejalan dengan semakin besarnya modul yang akan dibuat maka semakin banyak pula modul-modul didalamnya. Strategi hubungan antar modul ini ialah :

- **Top Down** – Dimana dalam strategi ini high level modul dibuat dan diintegrasikan lebih dahulu sebelum low level modul. Keuntungan pendeketai ini adalah kerusakan pada level ini yang umumnya sangat serius akan ketahuan duluan, sedangkan keburukannya ialah testing program akan sulit ketika modul low level membuat fungsi input-output (berhubungan ke high level modul).
- **Botton Up** – Kebalikan dari atas yaitu duluan low level modul yang dikerjakan dan di integrasikan. Keuntungannya ialah low level modul yang sudah selesai akan dapat digunakan atau dimodifikasi untuk modul ini. Kelemahannya akan sulit mengawasi operasi secara keseluruhan.
- **Threads** – Dengan pendekatan ini maka fungsi program yang paling penting yang duluan dibuat beserta modul-modulnya. Keuntungannya ialah fungsi yang paling penting duluan siap. Kelemahannya ialah integrasi dengan modul-modul yang lain akan lebih sulit dari dua pendekatan sebelumnya.

Tahap Testing – Tahap ini ditujukan untuk mengidentifikasikan adanya kesalahan, bukan ketidakberdayaan kesalahan. Tahap-tahap umum yang ditempuh biasanya adalah (1) Memilih batasan pengujian (2) Menentukan sasaran pengujian (3) Memilih pendekatan pengujian (4) Mengembangkan pengujian (5) Melakukan Pengujian (6) Mengevaluasi pengujian dan (7) Mendokumentasikan pengujian.

Jenis-Jenis Pengujian/Testing – Cukup banyak jenis pengujian yang biasanya dilakukan pada tahap ini, antara lain adalah :

- **Unit Testing**
- **Integration Testing**
- **Whole of Program Testing**

Tahap Operasi dan Pemeliaharann – Beberapa aktifitas utama pada tahap ini yang perlu dievaluasi oleh auditor adalah monitoring kenerja dan jenis-jenis pemeliaharaan dan perbaikan yang dilakukan serta pengedalian perangkat lunak manajemen konfigurasi yang digunakan.

Computar Operasional Control

Operation Control – Pengendalian ini nenentukan apakah fungsi manusia atau operasi otomasi yang harus dilakukan. Banyak jenis aktiviatas yang harus dilakukan untuk mendukung jalannya program di komputer, contohnya : program-program harus dijalankan ataupun dihentikan, media penyimpanan harus di isi dengan data yang up-to-data, berbagai formulir dan dokumen harus di cetak di printer dan lain sebagainya.

Di jaman yang modern ini ada juga kemungkinan penggunaan automated operations facilities (AOFs) yang melakukan semua pekerjaan manual diatas secara otaomtis. Campur tangan manusi akan menjadi semakin kecil jika sudah menggunakan AOFs ini.

Jenis – jenis operasi diatas tersebut adalah operasi normal dari komputer. Ketika semakin banyak operasi komputer dilakukan secara terotomatisasi, auditor harus menitikberatkan pemeriksaan pada masalah-masalah authentifikasi, akurasi, dan kelengkapan dari program yang berjalan terotomatisasi tersebut.

Scheduling Control – Pengendalian ini yang menentukan bagaimana sebuah pekerjaan harus dijadwalkan dalam lingkungan platform perangkat keras dan lunak. Inti dari pengendalaian ini ialah untuk memastikan bahwa sumber daya hardware yang dimiliki oleh perusahaan digunakan hanya oleh personil yang berhak dan juga hanya digunakan untuk kepentingan perusahaan semata.

Seorang auditor sebaiknya memeriksa eksistensi dan skedeul-skedul dari operasi perusahaan. Jika skedul ini belum ada atau kalaupun ada tiak selalu dipatuhi, maka titik berak pemeriksaan akan difokuskan dalam bagaimana mengefektifkan dan mengefisienkan skedul tersebut.

Maintenance Control – Pengendalian ini yang menentukan bagaimana perangkat keras harus dipelihara. Pemeliharaan hardware komputer adalah merupakan tindakan untuk mencegah kerusakan, sedangkan Perbaikan adalah usaha untuk memfungsikan kembali hardware yang sudah lebih dahulu rusak.

Perhatian utama auditor dalam hal pemeliharaan hardware adalah efektifitas dan efisiensi. Jika hardware tidak dapat diandalkan, output yang diharapkan juga tidak akan sesuai dengan yang diharapkan.

Nama : Laiatur Rahmi

Nim :182420118

Mata Kuliah : IT AUDIT

Dosen : Dr. Widya Cholil

Pada umum nya terdapat empat langkah utama dalam proses control (pengendalian) dalam suatu sistem audit

Langkah-langkah Audit Teknologi Informasi adalah sebagai berikut :

1. Identifikasi dan dokumentasi

Layaknya audit umum, identifikasi dan dukumentasi adalah keharusan. Hal ini bisa dilakukan dengan menjalankan survei maupun observasi ke lapangan sehingga audit bisa lebih objektif dan akurat.

2. Tes subtantif

Tes substansi merupakan tes yang dijalankan untuk mengetahui “isi” secara lebih mendalam. Dalam tes ini ada dua tipe yang bisa dijalankan: signifikan alias ditelusur secara lebih mendalam; atau terbatas.

3. Evaluasi

Setelah melakukan tes substantif, audit TI bisa menjalankan evaluasi berdasarkan hasil temuan. Di tahap ini kembali dicek apakah kinerja perusahaan efektif atau tidak. Kalau efektif berarti memenuhi syarat untuk dilanjutkan ke tahap selanjutnya. Namun kalau tidak efektif, lakukan lagi tes substantif.

4. Penilaian Mutu/ Kesimpulan

Di langkah terakhir ini akan terlihat apakah mutunya terjamin atau tidak. Jelas audit TI bukanlah tindakan yang bisa dilakukan secara asal dan instan. Ketelitian auditor menjadi ujung

tombaknya. Selain itu tentu saja, tujuan dan langkah-langkah tersebut harus dilakukan secara konsekuen.

Selanjutnya Selama audit TI, aktivitas -aktivitas dan prosedur yang dilaksanakan di antaranya adalah :

1. meninjau dokumentasi proses bisnis,
2. mengevaluasi kontrol yang tertanam dalam aplikasi seperti sistem *enterprise* (misal: sistem *enterprise resource planning, customer relationship management,* atau *supply chain management*),
3. menguji antarmuka antara sistem-sistem ini, meninjau *audit log* dari pemrosesan transaksi,
4. menguji akurasi dan validitas data yang tersimpan dalam basis data,
5. meninjau dan menguji kontrol akses terhadap aplikasi, basis data, dan jaringan, dan
6. mengevaluasi status proyek pengembangan sistem.

Berdasarkan referensi yang ada berikut proses control dalam hal pengembangan sistem , pemrograman dan operasional

1. Pengembangan Sistem
   a) Melakukan pendekatan audit.
      Ada beberapa pendekatan audit yang bisa dipilih auditor :
      - Membantu tim pengembangan meningkatkan kualitas sistem pengembangannya (Concurrent Audit)
      - Mengevaluasi sistem setelah selesai tahap proses pengembangan untuk menentukan apakah sisten tersebut apakah akan dihentikan, dilanjutkan atau dimodifikasi (Post Implementation Audit)
      - Menilai pengembangan sistem secara keseluruhan untuk mengurangi banyaknya *substantive test* yang dilakukan dalam menyatakan pendapat (General Audit)
   b) Melakukan evaluasi Pengembangan Sistem
      - Defenisi permasalahan, untuk memastikan apakah perusahaan *(stakeholders)* mengetahui apa resiko dan peluang yang mungkin terjadi terkait dengan penambahan suatu sistem informasi tersebut.

- Manajemen perubahan, dengan menitikberatkan pada mempersiapkan perubahan dalam perusahaan dengan pendekatan mendidik *unfreezing the organization)*; berubah ke sistem yang baru *(moving the organization)*; menolong siapa saja yang berkaiatan dengan sistem utnutk beradaptasi dan merasa nyaman dengan sistem yang baru ini *(refreezing the organization)*
- Studi kelayakan

  Perlu dilakukan untuk memperoleh komitmen perubahan dari seluruh bagian yang bakal berubah dan mempelajarai secara *cost-effective* apakah perubahan ini bisa dilakukan atau tidak, dan memastkan tidak akan menimbulkan permasalahan dikemudian hari. Ada 4 studi kelayakan yang erlu dilakukan perusahaan yaitu : technical feasibiity, operational feasibility, economic feasibilty, behavioral feasibility.
- Analisa sistem yang ada

  Jika sistem yang baru akan direkomendasikan untuk menggantikan sistem yang ada maka ada bebeapa hal yang perlu dilakukan perusahaan yaitu : mempelajari latar belakang, struktur dan budaya organisasi yang ada sekarang untuk mendapatkan pemahaman yang matang; mempelajari arus produk dan informasi yang akan diusulkan sis sietem yang baru.
- Menyusun kebutuhan strategis
- Mendesain organisasi dan pekerjaan
- Mendesain sistem pemrosesan informasi, dengan memeriksa enam aktifitas utama, yaitu :
  1. Pendeskripsian kebutuhan strategis untuk meminimalisir ketidakpastian di sekeliling sistem
  2. Memastikan bahwa hasil sistem ini memang benar-benar seperti yang diharapkan dan sesuai rencana
  3. Mengevaluasi keputusan dalam ruang lingkup database untuk mendefenisikan hal tersebut akan dilaksanakan atau tidak
  4. Memastikan pakah desainer sudah mengikuti suatu standar yang berhubungan dengan bagaimana membuat suatu desain yang baik
  5. Menitikberatkan perhatian apakah gambaran fisik desain sudah cukup baik atau tidak

6. Memastikan agar desain yang dibuat bisa terintegrasi dengan baik dengan *hardware* atau *software* yang sudah ada.

- Akuisisi/Pengembangan aplikasi
- Akuisisi perangkat lunak
- Pengembangan prosedur
- Uji penerimaan
- Konversi dan implementasi
- Operasi dan pemeliharaan

2. Manajemen Pemrograman

- Memahami dan fokus pada karakteristik program berkualitas tinggi, pengendalian manajemen pemrograman seperti : gunakan staf pemrograman berkualitas tinggi. Lakukan pemisahan fungsi, batasi kewenangan programer, dan hal penting lainnya.
- Evaluasi atas manajemen pemrograman

  Terdiri dari beberapa tahap, yaitu :

  1. Perencanaan . Sebagai auditor harus mengevaluasi apakah tingkt perencanaan sudah cukup dalam setiap usulan aplikasi yang direncanakan dan harus memastikan seberapa baikkah perencanaan kerja tersebut dilaksanakan.
  2. Desain. Auditor harus mengetahui alasan dan memastikan mengapa programmer menggunakan psuatu pendekatan desain model tertentu.
  3. Coding. Dimana programmer malekukan penulisan program yang pada akhirnya akan membuat program itu menjalankan perintah yang kita inginkan.
  4. Testing. Ditujukan untuk mengidentifikasikan adanya kesalahan, dengan menggunakan tahapan umum, yaitu : memilih batasan pengujian, menentukan sasaran pengujian, memilih pnedekatan penggujian, mengembangkan pengujian, melakukan pengujian, mengevaluasi pengujian, dan mendokumentasikan pengujian.
  5. Opersi dan pemeliharaan. Auditor memonitoring kinerja dan jenis-jenis pemeliharaan dan perbaikan yang dilakukan serta pengendalian perangat lunak manajemen konfigurasi yang digunakan.

3. Manajemen Operasional
    - Computer Operational Control. Terdiri dari : **operation control** (untuk menentukan apakah fungsi manusia atau operasi otomasi yang harus dilakukan); **schedulling control** (untuk memastikan ahwa sumber daya hardware yang dimiliki oleh perusahaan digunakan hanya oleh personil yang berhak dan hanya digunakan untuk kepentingan perusahaan saja; **maintenance control** (menentukan bagaimana perangkat keras harus dipelihara untuk mencegah kerusakan dan memfungsikan kembali hardware yang rusak.
    - Network Operation Control. Terdiri dari LAN controls dan WAN Controls. LAN controls berhubungan dengan kegiatan di Local Area Network, dimana manajemen operasi dalam LAN terjadi melalui fasilitas-fasilitas yang diberikan oleh file server. Wan controls merupakan pengendalian jaringan dalam lingkungan yang lebih luas. Ada suatu keadaan dimana operator harus mengidentifkasi kejadian tertentu dan mengkonfigurasi ulang jaringan untuk mengatasi masalah. Alat yang biasanya berguna untuk jaringan bersar ini disebut Network Control Terminal (NCT) dimana hanya hanya operator senior yang terlatih baik yang akan melaksanakan pengendalian guna menjaga keamanan aset dan integritas data dalam NCT.
    - Data Preparation dan Entry

      Meliputi :

      1. Source document design, dimana sebuah sumber dokumen terstruktur dengan baik, data apa saja yang dicatat, siapa yang mencatat, atau bagaimana dokumen tersebut disimpan ke dalam sistem.
      2. Source document storage, dimana sumber yang telah dientry diberi tanda dan tidak boleh dientry kembali dan dikendalikan dengan baik penyimpananya
      3. Inpput screen design, dimana perancangan tampilan layr input disesuaikan dengan dokumen sumber dan meperhatikan kemudahan pengguna dan kecepatan entry data.
      4. Data entry area design, dimana desain area pemsukan data harus embuat nyaman operator.
    - Production control. Meliputi receipt & dispatch of input &output, job schedulling, user service level agreement, transfer pricing or charge out control dan computer consumables.

- File library control. Bertanggung jawab terhadap pengorganisasian penggunaan media penyimpanan, seperti storage of storage media, use of storage media, maintenance and disposal of storage media, location of storage media.
- Documentation and program library control. Auditor dapat mengevalusi dengan menanyakan pada *documentation librarians* tetang tugas mereka, bagaiaman mereka mengorganisir penyimpanan dokumentasi danmemeriksa serta memastikan pencatatan dokumentasi berada dalam tempat yang aman sehingga orang yang tidak bertanggung jawab tidak bisa merubah dan memanfaatkan dokumentasi tersebut.
- Helpdesk/technical support control. Yang berfungsi : membantu end-user menggunakan hardware dan software, menyediakan dukungan y=teknis bagi sistem produksi dengan membantu memecahkan permasalahan.
- Mengevaluasi profil kinerja akan adanya aktifitas yang tidak terotorisasi. Auditor mengevaluasi bagaimana manajemen operasi menorganisir perencanaan kapasitas dan fungsi monitor performance. Akan lebih baik jika tersedia catatan statistik mengenai monitor pekerjaan mereka.
- Management of outsourced operations controls.

  Ada 4 pengendalian jika suatu perusahaan akan melakukan outsourcing, yaitu :

  1. Evaluasi atas kemampuan finansial vendor
  2. Memastikan ketaatan terhadap termin dan kondisi kontrak
  3. Memastikan kemampuan untuk mengendalikan operasi vendor
  4. Menjaga disaster recovery planning

Nama : Muhammad Angga Oktaharisetia

Nim : 182420123

IT AUDIT

1. TI Dalam peningkatan Pengendalian Internal

Kebanyakan entitas, termasuk bisnis kecil yng dimiliki keluarga berdasar pada TI untuk mencatat dan memproses transaksi bisnis. Sebagai hasil kemajuan luar biasa dalam di dalam TI, bahkan bisnis yang relatif sederhana menggunakan komputer pribadi dengan perangkat lunak akuntansi yang dibeli untuk proses akuntansi mereka. Penggunaan lingkungan jaringan yang kompleks, internet dn fungsi TI terpusat adalah umum dalam bisnis saat ini. Beberapa perubahan pengendalian internal yang diakibatkan oleh pengintegerasian TI ke dalam sistem akuntansi :

a. Kendali komputer menggantikan kendali manual.

   Mamfaat yang nyata dari TI, seperti kemampuan untuk menangani volume yang luar biasa dari transaksi bisnis yang rumit secara hemat biaya, menyebabkan organisasi untuk menggunakan TI sepanjang proses pelaporan keuangan mereka. Satu keuntungan TI adalah kemampuan untuk meningkatkan pengendalian internal dengan menggabungkan kendali yang dilakukan komputer dalam aktivitas proses transaksi sehari-hari. Menggantikan prosedur manual dengan pengendalian yang diprogramkan yang menggunakan cek dan saldo bagi masing-masing transaksi yang diproses dapat mengurangi kesalahan manusia yang mungkin terjadi dalam lingkungan manual yang tradisional. Suatu sistem TI yang terkendali menawarkan potensi lebih besar untuk mengurangi salah saji karena komputer memroses informasi secara konsisten. Contoh dari pengendalian internal yang dilakukan oleh komputer yang pernah diproses oleh karyawan sedang membandingkan pelanggan dan nomor produk dengan arsip induk dan membandingkan jumlah transaksi penjualan dengan batas kredit yang telah diprogram. Pengendalian keamanan online dalam aplikasi, data-base, dan sistem operasional juga menyediakan peluang untuk meningkatkan pemisahan dari kewajiban.

b. Tersedianya informasi dengan mutu lebih tinggi.

   Sekali manajemen yakin tentang keandalan informasi yang dihasilkan oleh TI, penggunaan manajemen atas informasi itu menawarkan potensi lebih lanjut untuk

meningkatkan keputusan manajemen. Pertama-tama, lingkungan TI yang kompleks umumnya diatur secara efektif karena kompleksitas memerlukan organisasi yang efektif, prosedur, dan dokumentasi. Kedua, sistem TI biasanya menyediakan bagi manajemen lebih banyak informasi dengan mutu lebih tinggi dengan lebih cepat dari kebanyakan sistem manual.

2. Resiko yang Muncul dari Penggunaan Sistem Akuntansi Berbasis TI

Meskipun IT meningkatkan pengendalian intern perusahaan, hal ini juga dapat mempengaruhi resiko-resiko pengendalian perusahaan secara keseluruhan. resiko khusus pada sistem TI yaitu:

1) Resiko pada perngkat keras

Meskipun IT memberikan manfaat pemrosesan yang signifikan, hal itu juga menciptakan resiko yang unik dalam melindungi perangkat keras dan data, termasuk potensi munculnya jenis kesalahan baru. Resiko khusus ini mencakup hal-hal berikut:

a. Ketergantungan pada kemampuan berfungsinya perangkat keras dan lunak.
b. Kesalahan sistematis versus kesalahan acak
c. Akses yang tidak sah salah
d. Hilangnya data

2) Jejak audit yang berkurang

Salah saji mungkin tidak terdeteksi dengan meningkatnya penggunaan IT akibat hilangnya jejak audit secara nyata , termasuk berkurangnya keterlibatan manusia. selain itu, computer juga menggantikan jenis otorisasi tradisional dalam banyak sistem IT.

a. Visibilitas jejak audit. karena sebagian besar informasi dimasukan secara langsung ke dalam computer, penggunaan IT sering kali mengurangi atau bahkan meniadakan dokumen dan catatan sumber yang memungkinkan organisasi menelusuri informasi akuntansi.
b. Keterlibatan Manusia yang berkurang. Dalam banyak sistem IT, karyawan yang terlibat dengan pemrosesan awal transaksi tidak pernah melihat hasil akhirnya. Karena itu, mereka kurang mampu mengidentifikasi salah saji pemrosessan, Walapun mereka melihat outout akhir, sering kali sulit untuk mengenali salah saji karena hasilnya sering sangat ringkas.
c. Tidak adanya otorisasi traditiona. Sistem IT yang sangat canggih biasanya diprakarsai jenis transaksi tertentu secara otomatis, seperti perhitungan bunga atas

rekening tabungan bank dan pemesanan persediaan apabila tingkat pesanan yang dtentukan telah dicapai,

3) Kebutuhan IT akan pengalaman dan pemisahan tugas

Sistem IT mengurangi sistem pemisahan tugas traditional (otorisasi, pembukuan, penyimpanan) dan menciptakan kebutuhan akan pengalaman IT tambahan.

3. Pengendalian Khusus atas Teknologi Informasi

Untuk menunjuk banyak dari risiko yang berhubungan dengan kepercayaan lebih besar atas TI, organisasi sering mengimplementasikan pengendalian khusus untuk fungsi TI. Standar audit menjelaskan dua pengelompokan pengendalian yang utama untuk sistem TI: pengendalian umum dan pengendalian aplikasi.

1) Pengendalian Umum (*General Control*), merupakan sistem pengendalian internal komputer yang berlaku umum dimana kegiatannya meliputi seluruh kegiatan komputerisasi sebuah perusahaan secara menyeluruh.

Auditor biasanya mengevaluasi pengendalian umum diawal audit oleh karena dampak dari pengendalian umum atas pengendalian aplikasi. Keenam kategori dari pengendalian umum kini diuji secara lebih detail. Keenam kategori tersebut adalah :

a. Administrasi dari Fungsi TI.
b. Pemisahan Tugas-tugas TI.
c. Pengembangan sistem.
d. Kemanan fisik dan online.
e. Backup dan Perencanaan Kontijensi
f. Pengendalian Perangkat Keras.

2) **Pengendalian Aplikasi** (*Application Control*), merupakan sistem pengendalian internal (*internal Controls*) pada sistem informasi berbasis teknologi informasi yang berkaitan dengan pekerjaan / kegiatan /aplikasi tertentu diamana setiap aplikasi mempunyai karakteristik tertentu dan kebutuhan pengendalian yang berbeda.

Pengendalian aplikasi dirancang untuk masing-masing aplikasi perangkat lunak dan dimaksudkan untuk membantu sebuah perusahaan memenuhi enam sasaran hasil audit yang terkait dengan transaksi. Walaupun beberapa pengendalian aplikasi mem-

pengaruhi satu atau hanya beberapa sasaran hasil audit yang terkait dengan transaksi, kebanyakan kendali mencegah atau mendeteksi beberapa jenis salah saji.

Pengendalian aplikasi bisa dilakukan oleh komputer atau oleh manusia. Pengendalian aplikasi yang dilakukan oleh manusia yang berinteraksi dengan komputer sering dikenal sebagai pengendalian pemakai. Efektivitas dari pengendalian pemakai, seperti tinjauan ulang dari laporan pengecualian yang dihasilkan-komputer, sering tergantung pada akurasi dari informasi yang dihasilkan. Pengendalian aplikasi terdiri dari tiga kategori, yaitu :

1. Pengendalian input
2. Pengendalian Pemrosesan
3. Pengendalian output

Pengendalian umum di-rancang untuk melindungi semua pengendalian aplikasi untuk memastikan bahwa pengendalian itu efektif. Pengendalian umum yang kuat mengurangi jenis risiko yang dikenali di kotak di luar bentuk oval pengendalian umum.

4. Dampak Teknologi Informasi Pada Proses Audit

Auditor harus memiliki banyak pengetahuan tentang pengendalian ini sebab mereka bertanggung jawab atas perolehan suatu pemahaman dari pengendalian internal, termasuk pengendalian umum dan pengendalian aplikasi, dengan mengabaik- an apakah penggunaan TI oleh klien adalah kompleks atau sederhana. Juga, pe- ngetahuan tentang pengendalian umum meningkatkan kemampuan auditor untuk ber- sandar pada pengendalian aplikasi efektif untuk mengurangi risiko pengendalian untuk sasaran hasil audit yang terkait dengan transaksi.

1) Pengaruh dari Pengendalian Umum oleh Risiko Pengendalian

Kebanyakan auditor mengevaluasi efektivitas dari pengendalian umum sebelum mengevaluasi pengendalian aplikasi. Jika pengendalian umumnya tidak efektif, ada potensi untuk salah saji material pada setiap aplikasi akuntansi yang berbasis komputer, dengan mengabaikan mutu dari pengendalian aplikasi.

Auditor biasanya memperoleh informasi tentang pengendalian umum dan aplikasi melalui wawancara dengan personil TI dan para pemakai kunci; pengujian dokumentasi sistem seperti bagan alur, manual pemakai, permohonan perubahan program, dan hasil

pengujian; dan tinjauan ulang dari daftar pertanyaan terperinci yang diselesaikan oleh staf TI. Dalam banyak kasus, diinginkan untuk menggunakan beberapa pendekatan dalam pemahaman pengendalian internal karena masingmasing menawarkan informasi yang berbeda. Wawancara dengan pejabat kepala informasi dan analis sistem menyediakan informasi yang bermanfaat tentang pengoperasian keseluruhan fungsi TI, tingkat dari pengembangan perangkat lunak dan perangkat keras yang dibuat untuk perangkat lunak aplikasi akuntansi kunci, dan suatu ikhtisar dari perubahan yang direncanakan. Tinjauan ulang dari program mengubah per- mintaan dan hasil percobaan sistem adalah bermanfaat dalam mengidentifikasikan perubahan program dalam perangkat lunak aplikasi. Daftar Pertanyaan berguna untuk mengidentifikasikan pengendalian internal yang spesifik.

2) Efek dari Pengendalian TI atas Risiko Pengendalian dan Ujian Substantif

Ingatlah dari bab sebelumnya bahwa auditor menghubungkan kekuatan dan kelemahan dalam pengendalian internal ke sasaran hasil audit yang terkait dengan transaksi yang spesifik. Berdasarkan pada kekuatan dan kelemahan itu, auditor menilai risiko pengendalian untuk masing-masing sasaran audit yang terkait dengan transaksi. Pendekatan yang sama itu digunakan dalam lingkungan TI, tetapi sekarang auditor mungkin mampu percaya pada pengendalian aplikasi yang dilakukan oleh komputer untuk mengurangi risiko pengendalian.

Auditor biasanya tidak menghubungkan kekuatan dan kelemahan dalam pe- ngendalian umum ke sasaran hasil audit yang terkait dengan transaksi yang spesifik. Seperti lingkungan pengendalian, pengendalian umum mempengaruhi sasaran hasil audit yang terkait dengan transaksi dalam beberapa siklus. Jika pengendalian umum tidak efektif, kemampuan auditor untuk percaya pada pengendalian aplikasi untuk mengurangi risiko pengendalian telah dikurangi. Dan sebaliknya, jika pengendalian umum adalah efektif, itu meningkatkan kemampuan auditor untuk percaya pada pe- ngendalian aplikasi untuk mengurangi risiko kendali.

Auditor mengidentifikasikan baik pengendalian manual dan pengendalian aplikasi yang dilakukan komputer dan kelemahan untuk masing-masing sasaran audit yang terkait dengan transaksi yang menggunakan suatu matriks risiko pengendalian dalam cara yang hampir sama seperti yang dibahas dalam bab sebelumnya.

3) Mengaudit dalam Lingkungan TI yang Tidak Terlalu Rumit

Banyak organisasi menggunakan TI untuk memroses transaksi bisnis dan merancang sistem tersebut sedemikian sehingga dokumen sumber dapat diperoleh kembali dalam format yang dapat dibaca dan dengan mudah bisa ditelusuri melalui sistem akuntansi ke keluaran. Dalam kejadian itu, banyak dokumen sumber yang tradisional seperti pesanan pembelian pelanggan, arsip pengiriman dan penerimaan, dan faktur penjualan dan pemasok. Perangkat lunak akuntansi yang terkait juga menghasilkan jurnal dan buku besar tercetak yang mengijinkan auditor untuk melacak transaksi individu melalui arsip akuntansi. Sebagai tambahan, pengendalian internal sering meliputi perbandingan klien atas arsip yang dihasilkan-komputer dengan dokumen sumber.

Dalam situasi ini, penggunaan TI tidak terlalu berdampak pada jejak audit. Biasa- nya, auditor memperoleh suatu pemahaman dari pengendalian internal dan melak- sanakan ujian dari pengendalian, ujian substantif transaksi, dan prosedur verifikasi saldo akun dengan cara yang sama seolah sistem akuntansi seluruhnya manual. Auditor masih bertanggung jawab untuk memperoleh suatu pemahaman dari pengen- dalian komputer umum dan aplikasi karena pengetahuan demikian bermanfaat dalam mengidentifikasikart risiko yang bisa mempengaruhi laporan keuangan. Namun, biasa- nya auditor tidak melaksanakan ujian pengendalian komputer. Pendekatan audit ini sering disebut mengaudit di sekitar komputer sebab auditor tidak menggunakan pengendalian komputer untuk mengurangi risiko pengendalian yang ditaksir.

4) Mengaudit dalam Lingkungan TI yang Lebih Rumit

Ketika organisasi memperluas penggunaan TI mereka, pengendalian internal sering ditanamkan di dalam aplikasi yang hanya terlihat dalam format elektronik. Ketika dokumen sumber yang tradisional seperti faktur, pesanan pembelian, arsip penagihan, dan arsip akuntansi seperti jurnal penjualan, daftar persediaan, dan catatan tambahan piutang dagang adalah hanya dalam format elektronik dibandingkan dengan aslinya (hard copy), auditor harus mengubah pendekatan ke audit. Pendekatan kepada audit ini sering disebut mengaudit melalui komputer.

Ada tiga kategori dari pengujian strategi ketika mengaudit melalui komputer: pendekatan data ujian, simulasi paralel, dan pendekatan modul audit tertanam.

a. Pendekatan Data Ujian. Pendekatan data ujian melibatkan pengolahan data ujian auditor menggunakan sistem komputer klien dan program aplikasi klien untuk menentukan apakah pengendalian yang dilakukan-komputer dengan tepat memproses data ujian itu. Karena auditor merancang data ujian itu, auditor bisa mengidentifikasi- kan materi ujian mana yang harus diterima atau ditolak oleh sistem klien. Auditor mem- bandingkan keluaran yang dihasilkan oleh sistem dari ujian data kepada keluaran yang diharapkan untuk menilai efektivitas dari aplikasi pengendalian internal program.

   Ketika menggunakan pendekatan data ujian, ada tiga pertimbangan auditor yang utama:

   a) Data ujian harus meliputi semua kondisi relevan yang ingin diuji auditor. Auditor harus merancang data ujian untuk menguji pengendalian kunci berbasiskomputer yang cenderung dipercayai auditor untuk mengurangi risiko pengendalian.
   b) Program aplikasi yang diuji oleh data ujian auditor harus sama dengan yang digunakan klien sepanjang tahun. Satu pendekatan adalah untuk menjalankan data ujian atas dasar kejutan, mungkin secara acak sepanjang tahun, walaupun melakukannya adalah mahal dan meng- habiskan waktu.
   c) Data ujian harus dihapuskan dari arsip klien. Jika uji coba perangkat lunak klien melibatkan data ujian pemrosesan selagi secara serempak memroses transaksi klien sebenarnya, auditor harus mengbilangkan data ujian di dalam arsip induk klien ketika pengujian selesai.

b. Simulasi Paralel. Berbagai perangkat lunak telah tersedia untuk membantu auditor dalam menentukan efektivitas pengendalian dalam perangkat lunak dan untuk memperoleh bukti tentang saldo akun yang dalam suatu format elektronik. Auditor rnenggunakan perangkat lunak yang dikontrol-auditor untuk melaksanakan operasional paralel kepada perangkat lunak klien dengan menggunakan arsip data yang sama. Ketiadaan perbedaan di dalam keluaran menunjukan perangkat lunak klien yang berfungsi secara efektif, sedangkan perbedaan menandai adanya kelemahan poten- sial. Sebab perangkat lunak auditor dirancang untuk memparalel suatu operasi yang dilakukan oleh perangkat lunak klien, strategi pengujian ini disebut pengujian simulasiparalel.

c. Pendekatan Modul Audit Tertanam. Saat menggunakan pendekatan modul audit tertanam, auditor memasukkan suatu modul audit dalam sistem aplikasi klien untuk menangkap transaksi dengan karakteristik yang menjadi minat spesifik auditor itu. Suatu keuntungan yang penting adalah kemampuan auditor menguji secara terus menerus, membandingkan dengan data ujian dan pendekatan simulasi paralel, yang dilaksanakan pada titik waktu tertentu. Keuntungan lain dari modul audit tertanam adalah kemampuan untuk mengidentifikasi semua transaksi yang tidak biasa untuk evaluasi auditor.

5. Masalah-Masalah Untuk Llngkungan TI Yang Berbeda

1) Masalah Untuk Lingkungan Komputer Mikro

Komputer mikro secara luas digunakan dalam banyak bisnis dengan mengabai-kan ukuran organisasi itu. Umumnya mereka memainkan suatu peran yang penting untuk bisnis yang kecil dalam memroses atau meneliti data akuntansi melalui penggunaan perangkat lunak akuntansi dan neraca lajur elektronik yang dibeli atau dibuat khusus.

Pengendalian umum dalam perusahaan yang lebih kecil pada umumnya sedikit kurang efektif dibanding dalam lingkungan TI yang lebih rumit. Seringkali, tidak ada IT personil yang khusus atau klien bersandar pada keterlibatan berkala konsultan TI untuk membantu dalam memasang dan memelihara perangkat keras dan lunak. Seringkali, auditor dari klien yang menggunakan komputer mikro dalam lingkung- an pengendalian umum yang tidak terlalu canggih melakukan sebagian besar audit mereka di sekitar komputer. Sistem ini sering menghasilkan jejak audit yang memadai yang mengijinkan auditor untuk merekonsiliasikan dokumentasi sumber masukan untuk keluaran.

Namun, bahkan dalam lingkungan TI yang tidak terlalu canggih, ada situasi di mana bisa bersandar pada pengendalian komputer. Sebagai contoh, program perangkat lunak dalam komputer mikro dapat diisikan pada hard-drive komputer dalam format yang tidak mengijinkan perubahan oleh personil klien. Risiko dari perubahan yang tidak sah di perangkat lunak kemudian menjadi rendah. Sebelum bersandar pada pengendalian yang dibangun ke dalam perangkat lunak tersebut, auditor harus mempunyai kepercayaan pada reputasi penjual perangkat lunak untuk mutunya.

Risiko lain dengan komputer mikro adalah bilangnya data dan program oleh karena virus komputer, yang dapat menyebar ke program lain dan sistem keseluruhan. Virus tertentu dapat merusak disk arsip atau menutup keseluruhan jaringan komputer. Memperbarui perangkat lunak pelindung virus secara teratur yang secara terus menerus menyaring penyebaran virus meningkatkan pengendalian.

2) Masalah Lingkungan Jaringan

Penggunaan jaringan yang makin meledak yang menghubungkan peralatan seperti komputer mikro, komputer jangkauan menengah, mainframe, stasiun kerja, server, dan pencetak sedang mengubah fungsi TI untuk banyak bisnis. Jaringan area lokal (Local Area Network/LAN) menghubungkan peralatan di dalam lingkungan bangunan yang kecil atau tunggal dan hanya digunakan untuk tujuan intra perusahaan. Penggunaan umum LAN adalah untuk memindahkan data dan program dari satu komputer atau stasiun kerja ke yang lainnya untuk mengijinkan semua alat untuk berfungsi bersama-sama. Jaringan Area Luas (WIde Area Network/WAN) menghubungkan peralatan dalam daerah geografis yang lebih besar, termasuk operasional global.

Dalam lingkungan jaringan, perangkat lunak aplikasi dan arsip data digunakan untuk memroses transaksi yang berada pada server, yang merupakan alat untuk mengolah data. Akses ke aplikasi dari komputer mikro atau stasiun-kerja diatur oleh perangkat lunak server jaringan. Perusahaan seringkali mempunyai beberapa server.

Saat klien mempunyai aplikasi akuntansi yang diproses dalam lingkungan jaring- an, pemahaman auditor akan pengendalian internal perlu meliputi pengetahuan konfi- gurasi jaringan, mencakup penempatan dan server, stasiun-kerja, dan komputer yang dihubungkan satu sama lain, dan pengetahuan perangkat lunak jaringan yang diguna- kan untuk mengatur sistem. Auditor juga harus memahami tentang pengendalian atas akses dan perubahan kepada program aplikasi dan arsip data yang ditempatkan pada server.

3) Masalah Sistem Manajemen Database

Auditor sering menghadapi aplikasi akuntansi yang menggunakan sistem manajemen database untuk memroses transaksi dan memelihara arsip data. Sistem manajemen database mengijinkan klien untuk menciptakan database yang berisi informasi yang dapat digunakan bersama dalam berbagai aplikasi. Dalam lingkungan non-database, masing-masing aplikasi berisi arsip data mereka sendiri, sedangkan dalam sistem manajemen database, banyak aplikasi berbagi arsip. Klien menerapkan sistem

manajemen database untuk mengurangi kelebihan data, meningkatkan pengendalian atas data, dan menyediakan informasi yang lebih baik untuk pengambilan keputusan dengan pengintegrasian informasi seluruh fungsi dan departemen. Sebagai contoh, data pelanggan, seperti alamat dan nama pelanggan, dapat digunakan bersama di fungsi penjualan, kredit, akuntansi, pemasaran, dan pengiriman, yang menghasilkan pengurangan biaya yang penting. Perusahaan sering mengintegrasikan sistem manajemen database ke seluruh organisasi. Program demikian disebut perangkat lunak perusahaan.

Kendali sering meningkat ketika data dipusatkan dalam sistem manajemen database dengan penghapusan arsip data yang berlebihan. Namun, sistem manajemen database juga dapat membuat risiko pengendalian internal. Sebagai contoh, ada risiko yang berhubungan dengan berbagai pemakai, mencakup individu di luar akuntansi, mengakses dan memperbarui arsip data. Tanpa administrasi database dan pengendalian akses yang tepat, risiko arsip data yang tidak sah, tidak akurat, dan tidak sempurna menjadi meningkat. Juga, pemusatan data ke dalam arsip tunggal meningkatkan pentingnya backup yang sesuai atas informasi data secara teratur.

Auditor dan klien yang menggunakan sistem manajemen database perlu memahami perencanaan klien, organisasi, dan kebijakan dan prosedur untuk menentukan seberapa baik sistem itu diatur.

4) Masalah Untuk Sistem E-commerce

Perusahaan yang menggunakan sistem e-commerce untuk melakukan transaksi bisnis secara elektronis menghubungkan sistem akuntansi internal mereka ke sistem yang dipelihara oleh pihak luar, seperti pelanggan dan pemasok. Sebagai hasilnya, risiko yang dihadapi suatu perusahaan saat terlibat dengan aktivitas e-commerce sebagian bergantung pada seberapa baik mitra e-commerce-nya mengidentifikasi dan mengatur risiko dalam sistem TI mereka sendiri. Untuk mengatur risiko interdependensi ini, perusahaan harus memastikan bahwa micra bisnis mereka secara efektif mengatur risiko sistem TI sebelum melaksanakan bisnis dengan mereka secara elektronis.

Penggunaan dari sistem e-commerce juga menyingkapkan data perusaha-an yang sensitip, program, dan perangkat keras terhadap pemotongan yang potensi atau sabotase oleh pihak luar. Untuk membatasi keterbukaan ini, perusahaan menggunakan firewalls, teknik pengkodean, dan tandatangan digital. Firewall melindungi data, program, dan sumber daya TI lain dari para pemakai eksternal yang mengakses sistem

melalui jaringan, seperti Internet. Firewall adalah suatu sistem dari perangkat keras dan lunak yang mengawasi dan mengendalikan aliran komunikasi e-commerce dengan penyaluran semua hubungan jaringan melalui suatu pintu gerbang pengendalian. Firewall dapat digunakan untuk memverifikasi pemakai eksternal dari jaringan, mem- berikan akses yang sah, dan mengarahkan pemakai ke program atau data yang di- minta.

Perusahaan menggunakan teknik pengkodean untuk melindungi keamanan komunikasi elektronik sepanjang proses transmisi. Teknik pengkodean didasarkan pada program komputer yang mengubah suatu pesan standar ke dalam suatu bentuk kode (encrypted). Penerima dari pesan elektronik itu harus menggunakan suatu program dekripsi (decryption) untuk memecahkan kode pesan itu. Seringkali teknik pengkodean kunci publik digunakan dimana satu kunci (kunci publik) digunakan E untuk menyandi pesan dan kunci yang lain (kunci pribadi) digunakan untuk memecah-kan kode pesan itu. Kunci publik dibagikan kepada pemakai yang disetujui dari sistem e-commerce itu dan hanya dapat digunakan untuk menyandikan pesan. Kunci pribadi, yang digunakan untuk memecahkan kode pesan, menjadi titik utama dari pengendali-an. Perlindungan kunci pribadi sering menjadi tanggung jawab dan administrator keamanan TI dan hanya dibagikan ke para pemakai internal dengan otoritas untuk memecahkan kode pesan itu.

Untuk membantu membuktikan keaslian kebenaran mitra dagang yang melaksa- nakan bisnis secara elektronik, perusahaan boleh bersandar pada otoritas sertifikasi eksternal yang memverifikasi sumber dari kunci publik melalui penggunaan tanda tangan digital. Suatu otoritas sertifikasi yang dipercaya mengeluarkan suatu sertifikat digital kepada individu dan perusahaan yang terlibat dalam e-commerce. Tanda tangan digital berisi nama pemilik dan kunci publiknya. Juga berisi nama dari otoritas sertifikasi dan tanggal tidak berlakunya sertifikat dan informasi khusus lainnya. Untuk menjamin keaslian dan integritas, masing-masing tandatangan secara digital ditandatangani oleh kunci pribadi yang dipelihara oleh otoritas sertifikasi.

5) Masalah Saat Klien Menggunakan Ti Pihak Luar

Banyak klien membuka beberapa atau semua kebutuhan TI mereka kepada pusat pelayanan komputer yang independen bukannya memelihara suatu pusat TI in-ternal. Banyak perusahaan yang lebih kecil membuka fungsi penggajian mereka ke pihak luar karena penggajian adalah cukup standar dari perusahaan ke perusahaan dan

di sana ada penyedia jasa penggajian yang dapat dipercaya. Perusahaan juga membuka sistem e-commerce mereka ke penyedia jasa situs Web eksternal. Seperti semua keputusan menggunakan pihak luar, perusahaan memutuskan apakah akan menggunakan TI pihak luar atas dasar manfaat-biaya.

Ketika menggunakan pusat jasa komputer pihak luar, klien menyerahkan data masukan, yang diproses oleh pusat jasa untuk suatu pembayaran (fee), dan mengembalikan keluaran yang telah disepakati dan masukan asli. Untuk penggajian, perusahaan menyerahkan kartu catatan waktu, tingkat upah, dan W4 kepada pusat jasa. Pusat jasa mengembalikan cek pembayaran upah, jurnal, dan data masukan setiap minggu dan W-2 pada akhir tiap tahun. Pusat jasa bertanggung jawab atas perancangan sistem komputer dan menyediakan pengendalian yang memadai untuk memastikan bahwa pemrosesan dapat dipercaya.

Auditor menghadapi suatu kesukaran ketika memperoleh suatu pemahaman dari pengendalian internal klien sebab banyak pengendalian itu berada di pusat jasa dan auditor tidak bisa berasumsi bahwa pengendalian adalah memadai hanya karena pusat jasa adalah suatu perusahaan independen. Standar audit meminta auditor untuk mempertimbangkan kebutuhan untuk memahami dan menguji pengendalian pusat jasa jika aplikasi pusat jasa melibatkan pemrosesan data keuangan yang penting.

Tingkat memperoleh pemahaman dan pengujian pengendalian pusat jasa harus didasarkan pada kriteria yang sama yang diikuti auditor dalam mengevaluasi pengendalian internal klien. Dalamnya pemahaman itu tergantung pada kompleksitas sistem dan tingkat dimana auditor berniat untuk menglirangi risiko pengendalian yang dinilai untuk mengurangi ujian audit substantif. Jika auditor menyimpulkan bahwa keterlibatan yang aktif dipusat jasa adalah satu-satunya cara melakukan audit, mungkin saja perlu untuk memperoleh suatu pemahaman akan pengendalian internal dipusat jasa dan menguji pengendalian menggunakan data ujian dan ujian pengendalian lainnya.

Dibeberapa tahun terakhir, makin menjadi umum untuk mempunyai auditor inde- penden memperoleh suatu pemahaman dan menguji pengengdalian internal dari pusat jasa untuk digunakan oleh semua pelanggan dan auditor independen mereka. Tujuan penilaian independen ini adalah untuk menyediakan pelanggan pusat jasa dengan suatu tingkat jaminan yang layak dari ketercukupan pengendalian umum dan aplikasi milik pusat jasa dan untuk menghapuskan kebutuhan akan audit yang berlebihan oleh auditor pelanggan. Jika pusat jasa mempunyai banyak pelanggan dan

masing-masing memerlukan suatu pemahaman dari pengendalian internal pusat jasa oleh auditor inde-penden mereka sendiri, kerepotan dan biaya untuk pusat jasa itu bisa besar. Ketika auditor independen pusat jasa menyelesaikan pemahaman dan uji coba atas pengendalian pusat jasa, maka dikeluarkan suatu laporan khusus, yang menunjukan lingkup dari audit dan kesimpulannya. Kemudian akan menjadi tanggung jawab dari auditor pelanggan untuk memutuskan tingkat dari kepercayaan pada pusat jasa. SAS 70 (AU 324) seperti dikembangkan oleh SAS 78 dan SAS 88 berisi bimbingan baik untuk auditor pelanggan dan auditor pusat jasa.

- https://mihok.my.id/pengendalian-internal-berkaitan-dengan-it/
- Sumber:http://www.coso.org/documents/internal%20controlintegrated%20framework.pdf.

- Sumber: https://www.isaca.org/popup/Pages/ApplicationControls.aspx.
- https://www.academia.edu/6530656/Auditing_-_TI

Nama : Mefta Eko Saputra
NIM : 182420113
Kelas : MTI 20A
Study : IT Audit

Proses Control & Pengendalian dalam Pelaksanaan Pengembangan Sistem

1. TOP MANAJEMEN

Manajemen Puncak dan Tata Kelola Perusahaan

Peran Dewan Komisaris

Komisaris adalah merupakan suatu pertahanan tyerakhir untuk memastikan antara manajemen puncak di sebuah perusahaan telah berkerja sebagai mana mestinya. Secara umum dalam suatu riteratur manajemen strategi dan tata laksana perusahaan, tugas – tugas pokok komisaris adalah sebagai berikut ;

a. Memonitor, komisaris harus selalu melihat perkembangan atau progress yang terjadi atas rencana strategis perusahaan. Bila perlu ia mendorong terjadinya percepatan untuk hal – hal tertentu
b. Mengevaluasi dan mempengaruhi, komisaris mempelajari usulan, keputusan dan tindakan manajemen; menyetujui atau tidak menyetujuinya, memberikan nasihat dan saran, atau menyampaikan tindakan alernatif.

Dengan peran – peran seperti di ata dengan demikian komisais juga mempunyai tanggungjawab dalam menentut arah perusahaan. Banyak negara – negera di dunia yang kini menganut asa bahwa tanggung jawab utama para komisaris adalah ;

a. Menginisiasi dan menentukan, komisaris dapat menentukan misi perusahaan dan menyatakan pilihan strategik pada manajemen.
b. Merekrut dan memberikan manajemen puncak
c. Mengontrol dan memonitor
d. Meninjau dan menyetujui penggunaan sumber daya
e. Memerhatikan kepentingan pemegang saham

Dalam prakteknya tugas ini belum berjalan atau di lakukan dengan baik oleh para komisaris. Ada komisaris yang memang sekedar pasang nama saja tanpa sedikit pun terlibat dalam urusan perusahaan. Sebaliknya, adajuga yang benar – benar aktif, mamantau dan memastikan perwujudan mis dan pencapainan visi perusahaan.

Anggota Dewan Komisaris

Pada sebagian perusahaan, anggota dewan komisarisnya biasanya adalah pihak – pihak yang memiliki hubungan dekat dengan pemegang saham. Pihak – pihak seperti ini sring di sebut dengan komisaris internal. Karena salah satu peranannya adalah untuk menjaga peranan pemegang saham, tentulah pertimbangan ini dapat di mengerti. Namun demikian, bila perusahaan itu sudah menjadu publik, di mana para pemegang saham sudah beragam. Adanya perdagangan itu di perlukan suatu komisaris eksternal, yang tidak lepas dari konsep " Agency theority, yaitu bahwa suatu masalah muncul di perusahaan karena manajamen puncak tidak mau bertanggung jawab atas keputusan mereka kecuali mereka memiliki jumlah saham yang cukup banyak di sebuah perusahaa. Artinya, dewan komisaris membutuhkan orang luar untuk menjamin agar manajeman puncak terhindar dari tidak mementngkan diri sendiri yang merugikan pemilik saham.

Uraian di atas berbeda dengan perdagangan yan di sebut sterwardship theory. Teori ini memiliki pandangan bahwa seseorang eksekutif junior, karena keterlibatannya dengan perusahaan, maka sebagian pihak internal, ia justru akan melindungi kepentingan perusahaan.

Peran Penting Komisaris

Alam banyak praktiknya para manajemen puncak seringkali sangat dominan dalam menentukan strategi dan implementasi strategi pada perusahaan, meskipun demikian, dewan komisaris pun pada dasarnya memiliki peran yang tidak bisa di abaikan, terutama terkait dengan penentua karakter dari derektur utamadan arah setrategi perusahaan. Dewan komisris mempunyai pran yang tidak kecil dari sudut pemilihan manajemen puncak ini.

Dalam teori " a theory of board directed strategik change" di cantumkan bahwa dewan komisaris pada dasarnya berperen signifikan, dalam ;

a. Menentukan perubahan strategik yang secara efektif dan selaras dengan strategi korporat.
b. Menggunakan suksesi direktur utama / CEO dengan merekut direktur utama dari luar untuk menginisiasi proses perubahan
c. Memilih direktur utama baru yang memiliki pengalaman sebelumnya dengan sterategi yang baru, yang nantinya akan di jalan kan.

Kombinasi dari pertimbangan strategi dan faktos psikologis dan membuat komisari memeilih direktur utama yang memiliki pengalaman dengan strtegi korporat, yang sejalan dengan strategi perusahaan sebelumnya.

Manajemen Puncak – Direktur Utama / CEO

Manajemen puncak adalah orang yang berperan dominan dalam perumusan strategik perusahaa. Mereka memeiliki tanggungjawab untuk mengarahkan tindakan yang akan merealisasikan rencana strategi yang sudah di rumuskan. Tanggung jawab direktur utama dan para direktur lainya, sering di anggp menjadi dua hal yang pokok, yaitu ;

a. Memimpin pelaksanaan misi dan memberikn visi strategic

   Memimpin melaksanakan misi di sini maksudnya adalah bahwa direktur utama mengarahkan semua aktifitas agar perusahaan mancapai tujuannya. Sedangakan, yang di maksud dengan visi strategi adalah gambaran terbaik tentang seperti apa seharusnya wujud perusahaan. Inilah yang sering di wujudkan dalam menyatakan visi dan misi perusahaan. Di mana di harapkan dimana sepuruh kariyawan merasa manjadi bagian dari misi dan visi tersebut. Hal tersbut baru akan tercipta jika para directur menunjukan menjadi contoh, dan menularkan ke pada seluruh karyawan. Paa pemimpin yang bersifat trasformatif ini pada dasarnya mampu membuat para karyawan berkerja untuk sesuatu yang lebih dari sekedar detail pekerjaan sehari – hari. Segala prilaku sikap dan nilai – nilai yang di anut, dan segala tindak – tanduk menjadi acuan dan di contoh oleh karyawan.

b. Mengelola Proses Perencanaan Strategi

   Manajemen puncak mempunyai peran penting dalam menyesuaikan proses perencanaan strategik perusahaan. Banyak sekali yang terjadi, rencana strategik yang sudah di rapatkan alam rapat – rapat perencanaan, dan di rumuskan untuk di laksanakan, tidak memperoleh hasil yang memadai, karena lemahnya pengelolaan manajemen puncak. Salah satu penyebab utamanya adalah peran perancanaan strategi tidak muncul dari unit – unit bisnis atau devisi – devisi dalam perusahaan. Pendekatan seperti ini di kenal dengan pendekatan bottom – up. Jadi, tidak Top – down, di mana rencana semuanya di rumuskan oleh manajemen puncak , sehingga pihak – pihak di unit bisns atau devisi sekedar melaksanakan saja. Manajeman puncak tidak memastikan aktivitas – aktivitas yang di jaankan sesuatu dengan rencana strategi secara

keseluruhan. Pengevaluasian yang di lakukan oleh manajemen pucak atas implimentasi dari rencna strategik, yang merupakan program dari departemen, devisi, atau unit usaha harus dengan baik.

Komisaris dan Direktur Dari Sudut Pandang UU Perseroan Terbatas

Di Indonesia, perturan mengenai tanggungjawab dan peran direksi serta komisaris, di atur dengan undang – undang nomor 40 tahu 2007, tentang perseroan terbatas. Dalam UU ini, di sebutkan bahwa komisaris dan direktur adalah organ PT, bersama denga rapat umum pemegang saham. Direksi di rumuskan di UU PT ini sebagai organisasiperseroan yang berwewenang dan bertanggung jawab penuh atas perusahaan perseroan untuk kepentingan perseroan sesuai dengan maksud dan tujuan perseroan serta mewakili perseroan baik di dalam maupun di luar pengendalian sesuai dengan ketentuan anggaran dasar. Dalam UU PT, ada unsur tugas memelihara, berhati – hati dalam mengambil keputusan dan pengendalian kondisi perusahaan.

Ini berarti pemilik perusahaan tidak akan semberangan dalam memilih direkturnya. Dalam praktiknya permasalahan terkait dengan komisaris sering kali terjadi, biasanya permasalahan yang muncul adalah ;

a. Tidak adanya pemisahan yang tegas antara direksi dan komisris

Meskipun asas pemisahan ini sudah jelas, namun masih banyak dalam praktiknya pemisahan tersebut tidak berjalan sebagai mana semestinya.

b. Komposisi ke anggotaan

Isu yang muncul dari permasalahan ini adalah menyangkut upaya memastikan agar komposisi keanggotaan komisaris dan direksi memungkinkan untuk dapat di capai pengambiln keputusan secara cepat, tepat, efisien, dan berimbang.

c. Proses nominasi yang tidak transparan

Selain harus memenuhi kreteria tertentu tersebut dalam proses penunjukan anggota komisaris dan direksi, perlu di lakukan melalui mekanisme yang formal

d. Rendahnya independensi

Rendahnya independensi yang merupakan suatu hal partama bagi komisris dalam menjalankan fungsinya, dapat mengekibatkan ia menjadi kurang objektif.

Prinsip – prinsip Tata Kelola Perusahaan

Ada lima prinsip yang kini banyak di sepakati yaitu ;

a. Transparasi, bahwa perusahaan harus menyediakan informasi yang memadai dan relevan serta dapat di akses para pemangku kepentingan
b. Akuntabilitas, perusahaan harus mempertanggung jawapkan kinerjanya secara transparan dan wajar, dan di kelolo secara ter ukur
c. Responsibilitas, perusahaan selakyaknya mengetahui aturan yang berlaku dan melaksanakan secara bertanggung jadwal
d. Independen, organ – organ yang ada dalam perusahaan tidak saling mendominasi
e. Kesetaaan dan kewajiban, bahwa perusahaan harus selalu memerhatikan kepentingan pemegang saham dan pemangku kepentingan berdasarkan asas ke setaraan.

Tahapan Manajemen Strategik

Pada prinsipnya, manajemen strategik terdiri atas tiga tahapan, yaitu:

Tahap Formulasi

Meliputi pembuatan misi, pengidentifikasian peluang dan tantangan eksternal organisasi, penentuan kekuatan dan kelemahan internal, pembuatan sasaran jangka panjang, pembuatan pilihan-pilihan strategi, serta pengambilan keputusan strategi yang dipilih untuk diterapkan. Dalam hal penyusunan strategi, Fred R. David membagi proses ke dalam tiga tahapan aktivitas, yaitu: input stage, matching stage, dan decision stage. Termasuk di dalam formulasi strategi adalah pembahasan tentang bisnis baru yang akan dimasuki, bisnis yang dihentikan, alokasi sumber-sumber yang dimiliki, apakah akan melakukan ekspansi atau diversifikasi usaha, apakah akan memasuki pasar internasional, apakah akan melakukan merjer atau membentuk joint-venture, serta bagaimana untuk menghindari pangambilalihan secara paksa (hostile takeover).

Tahap Implementasi

Meliputi penentuan sasaran tahunan, pengelolaan kebijakan, pemotivasian pegawai, pengalokasian sumber-sumber agar strategi yang diformulasikan dapat dilaksanakan. Termasuk di dalamnya adalah pengembangan kultur yang mendukung strategi, penciptaan struktur organisasi yang efektif, pengarahan usaha-usaha pemasaran, penyiapan anggaran, pengembangan dan pemanfaatan sistem informasi, serta mengkaitkan kompensasi pegawai

dengan kinerja organisasi.[bandingkan dengan Senge, 1994]. Pada tahap ini, ketrampilan interpersonal sangatlah berperan. Sebagaimana Carl von Clausewitz (1780-1831) dalam bukunya yang diterbitkan kembali On War, strategi bukanlah sekedar aktivitas problem-solving, tetapi lebih dari itu strategi bersifat terbuka (open-ended) dan kreatif untuk mempertajam masa depan dalam model chain of command di mana suatu strategi harus dijalankan setepat mungkin (menghindari bias-bias yang tidak perlu dalam setiap bagian struktur organisasi).

Tahap Evaluasi

Meliputi kegiatan mencermati apakah strategi berjalan dengan baik atau tidak. Hal ini dibutuhkan untuk memenuhi prinsip bahwa strategi perusahaan haruslah secara terus-menerus disesuaikan dengan perubahan-perubahan yang selalu terjadi di lingkungan eksternal maupun internal. Tiga kegiatan utama pada tahap ini adalah: (a) menganalisa faktor-faktor eksternal dan internal sebagai basis strategi yang sedang berjalan; (b) pengukuran kinerja; (c) pengambilan tindakan perbaikan

PENGEMBANGAN SYSTEM

Audit Pengembangan Sistem Dalam Tata Kelola IT

Audit merupakan sebuah kegiatan yang melakukan pemerikasaan untuk menilai dan mengevaluasi sebuah aktivitas atau objek seperti implementasi pengendalian internal pada sistem informasi akuntansi yang pekerjaannya ditentukan oleh manajemen atau proses fungsi akuntansi yang membutuhkan improvement. Proses auditing telah menjadi sangat rapi di Amerika Serikat, khususnya pada bidang profesional accounting association. Akan tetapi, baik profesi audit internal maupun eksternal harus secara terus menerus bekerja keras untuk meningkatkan dan memperluas teknik, karena profesi tersebut akan menjadi tidak mampu untuk mengatasi perkembangan dalam teknologi informasi dan adanya tuntutan yang semakin meningkat oleh para pemakai informasi akuntansi. Meskipun berbagai macam tipe audit dilaksanakan, sebagian besar audit menekankan pada sistem informasi akuntansi dalam suatu organisasi dan pencatatan keuangan dan pelaksanaan operasi organisasi yang efektif dan efisien. Secara garis besar perlunya pelaksanaan audit dalam sebuah perusahaan yang telah mempunyai keahlian dalam bidang teknologi informasi yaitu antara lain:

A. Kerugian akibat kehilangan data.

   Data yang diolah menjadi sebuah informasi, merupakan aset penting dalam organisasi bisnis saat ini. Banyak aktivitas operasi mengandalkan beberapa informasi yang penting. Informasi sebuah organisasi bisnis akan menjadi sebuah potret atau gambaran dari kondisi organisasi tersebut di masa lalu, kini dan masa mendatang. Jika informasi ini hilang akan berakibat cukup fatal bagi organisasi dalam menjalankan aktivitasnya.

B. Kerugian akibat kesalahan pemrosesan komputer.

   Pemrosesan komputer menjadi pusat perhatian utama dalam sebuah sistem informasi berbasis komputer. Banyak organisasi telah menggunakan komputer sebagai sarana untuk meningkatkan kualitas pekerjaan mereka. Mulai dari pekerjaan yang sederhana, seperti perhitungan bunga berbunga sampai penggunaan komputer sebagai bantuan dalam navigasi pesawat terbang atau peluru kendali. Dan banyak pula di antara organisasi tersebut sudah saling terhubung dan terintegrasi. Akan sangat mengkhawatirkan bila terjadi kesalahan dalam pemrosesan di dalam komputer. Kerugian mulai dari tidak dipercayainya perhitungan matematis sampai kepada ketergantungan kehidupan manusia.

C. Pengambilan keputusan yang salah akibat informasi yang salah. Kualitas sebuah keputusan sangat tergantung kepada kualitas informasi yang disajikan untuk pengambilan

keputusan tersebut. Tingkat akurasi dan pentingnya sebuah data atau informasi tergantung kepada jenis keputusan yang akan diambil. Jika top manajer akan mengambil keputusan yang bersifat strategik, mungkin akan dapat ditoleransi berkaitan dengan sifat keputusan yang berjangka panjang. Tetapi kadangkala informasi yang menyesatkan akan berdampak kepada pengambilan keputusan yang menyesatkan pula.

Dampak dari kejahatan dan penyalahgunaan komputer tersebut antara lain:

- Hardware, software, data, fasilitas, dokumentasi dan pendukung lainnya rusak atau hilang dicuri atau dimodifikasi dan disalahgunakan.
- Kerahasiaan data atau informasi penting dari orang atau organisasi rusak atau hilang dicuri atau dimodifikasi.
- Aktivitas operasional rutin akan terganggu.
- Kejahatan dan penyalahgunaan komputer dari waktu ke waktu semakin meningkat, dan hampir 80% pelaku kejahatan komputer adalah orang dalam.

Tujuan dan Lingkup Audit Sistem Informasi

Tujuan Audit Sistem Informasi dapat dikelompokkan ke dalam dua aspek utama, yaitu:

- Conformance (Kesesuaian) – Pada kelompok tujuan ini audit sistem informasi difokuskan untuk memperoleh kesimpulan atas aspek kesesuaian, yaitu : Confidentiality (Kerahasiaan), Integrity (Integritas), Availability (Ketersediaan) dan Compliance (Kepatuhan).
- Performance (Kinerja) - Pada kelompok tujuan ini audit sistem informasi difokuskan untuk memperoleh kesimpulan atas aspek kinerja, yaitu : Effectiveness (Efektifitas), Efficiency (Efisiensi), Reliability (Kehandalan).

Tahap – Tahap Dalam Audit Teknologi Sistem Informasi

1. Tahap Pemeriksaan pendahuluan

Sebelum auditor menentukan sifat dan luas pengujian yang harus dilakukan, auditor harus memahami bisnis auditi (kebijakan, struktur organisasi, dan praktik yang dilakukan). Setelah itu, analisis resiko audit merupakan bagian yang penting dan berusaha untuk memahami pengendalian terhadap transaksi yang diproses oleh aplikasi tersebut.

Pada tahap ini pula auditor dapat memutuskan apakah audit diteruskan atau mengundurkan diri dari penugasan audit.

2. Tahap Pemeriksaan Rinci

Pada tahap ini auditnya berupaya mendapatkan informasi lebih mendalam untuk memahami pengendalian yang diterapkan dalam sistem komputer klien. Auditor harus dapat memperkirakan bahwa hasil audit pada akhirnya harus dapat dijadikan sebagai dasar untuk menilai apakah struktur pengendalian intern yang diterapkan dapat terpercaya atau tidak. Kuat atau tidaknya pengendalian tersebut akan menjadi dasar bagi auditor dalam menentukan langkah selanjutnya.

3. Tahap Pengujian Kesesuaian

Dalam tahap ini, dilakukan pemeriksaan secara terinci saldo akun dan transaksi Informasi yang digunakan berada dalam file data yang biasanya harus diambil menggunakaan software CAATTs(Computer Assisted Audit Tools and Techniques). Dengan kata lain, CAATTs digunakan untuk mengambil data untuk mengetahui integritas dan kehandalan data itu sendiri.

Sejarah

Audit teknologi sistem informasi pada awalnya lebih dikenal sebagai EDP Audit (Electronic Data Processing) telah mengalami perkembangan yang pesat. Perkembangan audit teknologi sistem informasi ini didorong oleh kemajuan teknologi dalam sistem keuangan, meningkatnya kebutuhan akan kontrol informasi teknologi, dan pengaruh dari komputer itu sendiri untuk menyelesaikan tugas penting. Sistem keuangan pertama yang menggunakan teknologi komputer muncul pertama kali tahun 1954. Selama periode 1954 sampai dengan 1960-an profesi audit masih menggunakan komputer. Pada pertengahan 1960-an terjadi perubahan pada mesin komputer, dari mainframe menjadi komputer yang lebih kecil dan murah. Pada tahun 1968, American Institute of Certified Public Accountants (AICPA) ikut mendukung pengembangan EDP auditing. Sekitar periode ini para auditor bersama-sama mendirikan Electronic Data Processing Auditors Association (EDPAA). Tujuan lembaga ini dibuat adalah untuk membuat suatu tuntunan, prosedur, dan standar bagi audit EDP. Pada tahun 1977, edisi pertama Control Objectives diluncurkan. Publikasi ini kemudian

dikenal sebagai Control Objectives for Information and Related Technology (CobiT). Tahun 1994, EDPAA mengubah namanya menjadi Information System Audit (ISACA).

Kesimpulan

Audit teknologi sistem infromasi adalah untuk menentukan apakah aset sistem informasi perusahaan itu telah bekerja secara efektif, dan integratif dalam mencapai target organisasinya. Alasan mengapa teknologi sistem informasi saat ini menggunakan audit karena didorong oleh kemajuan teknologi dalam sistem keuangan, meningkatnya kebutuhan akan kontrol informasi teknologi, dan pengaruh dari komputer itu sendiri untuk menyelesaikan tugas penting. Ada 5 jenis tipe dari audit teknologi sistem informasi yaitu sistem dan aplikasi, fasilitas pemrosesan informasi, pengembangan sistem, arsitektur perusahaan dan manajemen TI, dan Client-server, telekomunikasi, intranet serta internet yang mendukung seluruh pekerjaan atau tugas dari audit teknologi sistem informasi.

PEMROGRAMAN

Manajemen Pemrogramman Dalam Tata Kelola IT

Manajemen pemrogramman dalam tata kelola it yaitu untuk melakukan evaluasi terhadap manajemen pemrograman, auditor juga ditutut untuk memahami dan memberikan perhatian ekstra pada beberapa karakteristik program yang berkualiatas tinggi. Berikut ini merupakan karakteristik program berkualitas tinggi :

- Berfungsi secara benar dan lengkap
- Mempunyai antarmuka pengguna yang berkualitas tinggi
- Bekerja secara efektif dan efisien
- Didesain dan didokumentasikan dengan baik
- Mudah untuk dilakukan pemeliharaan
- Bisa beradaptasi pada kondisi abnormal

Beberapa hal penting dalam pengendalian manajemen pemrograman antara lain:

- Memiliki staff dengan pengetahuan yang tinggi
- Memisahkan fungsi-fungsi
- Mengembangkan dan membuat dokumentasi terhadap metodologi dan standar kerja
- Membatasi kewenangan programmer
- Memiliki log manual dan log aktivitas programmer
- Memiliki konsultan luar untuk melakukan evaluasi
- Memberikan penilaian atas kinerja programmer secara berkala

Tahapan manajemen pemrogramman untuk melakukan evaluasi :

- Tahapan perencanaan

  Pada tahapan ini auditor perlu detail terhadap hal-hal teknis dan non teknis, misalnya pada biaya pemrogramman. Sehingga mampu mengendalikan cost dan kebutuhan lainnya.
- Tahapan Desain

  Dalam tahanap ini untuk era sekarang dulu pekerjaan ini dilakukan oleh seorang programmer namun saat ini programmer terbantu dengan adanya UI/UX desainer yang mampu dan lebih paham untuk mencari struktur dan output yang dihasilkan namun tidak melupakan juga untuk lebih banyak berdiskusi dengan programmer. Auditor juga harus paham dari kedua sisi yang berbeeda ini.

- Tahapan Coding

  Tahapan ini programmer melakukan penulisan code program yang pada akhirnya akan menghasilkan output dari program itu sendiri dan menjalankan perintah sesai dengan apa yang kita inginkan. Pada bagian ini juga tak lupa untuk melakukan penyusunan terhadap modul-modul pekerjaan agar lebih mudah untuk dikerjakan.

- Tahapan Testing

  Tahapan ini ditunjukan untuk mengidentifikasikan adanya bugs ataupun kesalahan – kesalahan yang ada. Tahapan ini juga memilikan hal – hal umum untuk ditempuh, biasanya adalah membatasi tahapan pengujian, memnentukan sasara pengujian, memilih pendekatan pengujian, mengembangkan pengujian, melakukan pengujian dan mengadakan evaluasi hingga mendokumentasikan pengujian.

- Tahapan operasi & Pemeliharaan

  Tahapan ini biasanya merupakan hal – hal yang sangat berkaitan pada evaluasi yang perlu dilakan oleh auditor, kegiatannya meliputi monitoring kinerja hingga jenis pemeliharaan dan perbaikan yang akan dilakukan kedepannya serta untuk melakukan manajemen konfigurasi perangkat lunak yang akan digunakan.

OPERASIONAL

Audit Operasional Dalam Tata Kelola IT Sifat Audit Operasional Tata kelola informasi

Satu tipe utama audit operasional meliputi pengauditan fungsi tata kelola informasi. Audit operasional tata kelola informasi secara sistematis memperkirakan keefektifan unit-unit dalam mencapai tujuan dan mengidentifikasikan kondisi yang dibutuhkan untuk perbaikan. Tata kelola informasi audit operasional mempunyai sifat yang luas meliputi semua kegiatan departemen Pemrosesan atau mungkin dihubungkan dengan segmen khusus dalam kegiatan tersebut, tergantung pada tujuan manajemen.

Situasi Yang Muncul Dalam Audit Operasional Tata kelola informasi

Dalam hal tata kelola informasi yang umumnya terjadi adalah:

1. Biayanya tinggi untuk penyediaan jasa komputer.
2. Bagian utama dari rencana perusahaan.
3. Usulan perolehan hardware yang utama atau meng-upgrade software.
4. Ketidakmampuan menerima tata kelola informasi komputer secara eksekutif.
5. Kebutuhan tata kelola informasi eksekutif yang baru untuk penilaian secara intensif.
6. Ketidakteraturan perputaran personil dalam departemen tata kelola informasi.
7. Usulan untuk mengkonsolidasi atau mendistribusikan sumberdaya tata kelola informasi.
8. Merupakan sistem utama yang tidak responsif terhadap kebutuhan atau sulit dalam pemeliharaan.
9. Meningkatnya jumlah komplain user.

Proses Audit Operasional Tata kelola Informasi

Audit planning phase

Audit operasional pada fungsi data processing tidak mempunyai starting place, tetapi berpedoman pada tujuan audit. Masing-masing audit mempunyai ciri khas dan memerlukan individual treatment karenanya lingkup audit berbeda sesuai dengan tujuannya.

Dengan mengabaikan lingkup audit, tugas pertama dalam audit operasional yaitu untuk memperkenalkan diri pada organisasi dan *Data Prossesing* (DP) departemen untuk

diaudit. Hal ini adalah sebuah tahap penting bagi auditor untuk memperoleh dan meninjau ulang latar belakang informasi pada unit, aktivitas, dan fungsi yang akan diaudit.Tahap ini penting dan sebaiknya diikuti dengan mengabaikan audit operasional yang dilakukan secara internal. auditor sebaiknya mengumpulkan informasi dari klien untuk memperoleh pemahaman tentang DP departemen dan tujuannya.

Banyak latar belakang informasi yang sebaiknya digunakan auditor pada tahap ini mencakup lokasi departemen DP, nama manajer pada DP, no SDM pada DP berdasar level dan tipe, metode evaluasi SDM, tingkat pertukaran SDM, tugas dan tanggung jawab karyawan, identifikasi peralatan komputer yang digunakan dan identifikasi sistem operasi yang digunakan. phisical layout chart pusat komputer sebaiknya diperoleh dari DP manajer (atau, jika tak tersedia, disiapkan oleh auditor). kerjasama DP manajemen menjadi hal yang penting selama tahap perencanaan.

Preliminary survey phase

Setelah tujuan audit tealah ditetapkan, dan lingkup audit telah ditentukan serta manajemen cooperation diperoleh, maka auditor siap untuk preliminary survey. survei membantu auditor untuk mengidentifikasi lingkup masalah, sensitive area, dan operasi yang rumit tentang audit DP departement. Setelah preliminary survey, auditor harus bisa menentukan tingkat kompleksitas audit operasional.selama preliminnary survey, auditor akan mempelajari permasalahan operasional manajemen DP. Auditor perlu mendalami mengenai DP center sehingga familiar dengan pengoperasiannya. Auditor sebaiknya membuat rencana dalam mengusulkan petunjuk DP centernya dan bertindak sebagai penghubung bagi semua data collection dan dokumentasi syang diperoleh. Auditor akan membentuk rencana tahapan dalam operasi actual yang disesuaikan dengan diskripsi tertulis maupun lisan dan pemahaman yang telah diberikan oleh DP personil kepada auditor. Proses verifikasi ini memerlukan contoh transaksi atau lingkup kerja yang diuji

secara detail. Prelimanary phase pada operational audit merupakan basis pada tahap pengujian audit yang terperinci. DP manajemen sebaiknya diberitahu pengungkapan penyimpangan dan membantu dalam petunjuk pada lingkup permasalahan. Auditor mendisain program audit untuk maenemukan pertimbangan atau penyebab ketidak cocokan.

Detailed audit phase

Aktivitas untuk menguji dan mengevaluasi tahap audit ini meliputi :

1. fungsi pengolahan informasi pada organisasi
2. praktek dan kebijakan sumber daya manusia
3. operasi komputer
4. pengembangan sistem dan implementasinya
5. aplication system operation

lima area terdaftar ini diharapkan dapat menyajikan beberapa faktor-faktor penting yang harus dipertimbangkan. ketika mereka memberi auditor suatu pandangan umum tentang komponen penting DP functioni dan dapat bertindak sebagai starting point yang baik.

Reporting

pada tahap penyelesaian opersional audit laporan diberikan kepada manajemen dan komite audit perusahaan.Isi dari laporan ini bervariasi sesuai pada harapan manajemen.contohnya : laporan mungkin terdiri dari pendapat yang mengacu pada fungsi pengelolaan informasi yang efektif dan efisien, dan saran-saran yang membangun.Internal auditor diwajibkan untuk melakukan follow up pada report audit findings dan memberikan rekomendasi untuk memastikan bahwa komite audit mengambil langkah yang tepat.

Audit Operasional

Ada tiga jenis audit operasional (Operational Audit), antara lain:

Post Implementation Audit Pelaksanaan post implementasi audit atau audi setelah implementasi ini dijalnakan oleh auditor dengan penerapan, pengalamannya dalam pengembangan sistem aplikasi, sehingga auditor dapat mengevaluasi apakah sistem yang diimplementasikan harus dimutakhirkan atau diperbaiki atau bahkan dihentikan apabila sudah tidak sesuai dengan keperluan atua mengandung kesalahan

Conccurrent Audit (Audit Bersama) Audit menjadi tim pengembang sistem, auditor membantu tim untuk melakukan peningkatan kualitas dikembangkannya sistem yang dibangun oleh analisis, desingner dan programmer dan akan diterapkan.

Concurrent Audits (Audit Secara Bersama-sama) Auditor melakukan evaluasi kinerja unit fungsional atau fungsi sistem informasi apakah telah dikelola dengan baik, apakah kontrol berkembangnya sistem secara menyeluruh sudah dijalankan dengan baik, apakah sistem kompute rsudah dikelola dan dioperasikan dengan baik.

Dalam melakukan audit sistem komputerisasi yang ada, dilaksanakan dengan menyeluruh, pada saat menjalankan pengujian, dimanfaatkan bukti menarik kesimpulan dan memberikan rekomentasi terhadap manajemen tentang hal yang berkaitan dengan efektititas, efisiensi dan ekonomisnya sistem.

Nama : **Miftahul Fallah**
Nim : **182420132**
Kelas : **MTI. 20A**
DosenPengasuh : **Dr Widya Cholil , S.Kom., M.I.T.**
Mata Kuliah : **IT Audit**

Soal

untuk proses control (pengendalian) ada tindakan yang perlu dilaksanakan, gunaka referensi yang ada untuk menjawap pertanyaan saya tertutama dalam hal pengembangan sistem, pemrogramaan dan operasional.

Jawaban

Pengendalian umum atau pengendalian manajemen adalah mengevaluasi aspek-aspek pengendalian umum pada TI apakah sudah dilakukan dengan baik oleh manajemen atau belum.

1. Pengembangan Sistem

Suatu hal yang menjadi perdebatan sejak dahulu ialah mengenai hal yang berfokus pada apakah seorang auditor sebaiknya terlibat dalam tim pengembangan selama proses pengembangan sistem.

a. Pendekatan audit pengembangan sistem

   Auditor dapat memilih salah satu atau kombinasi dari tiga pendekatan berikut ini:

   - Concurrent Audit , Auditor merupakan bagian dari tim pengembangan sistem. Tugas mereka ialah membantu tim pengembangan meningkatkan kualitas sistem pengembanganny.
   - Post implementation Audit, auditor melakukan audit setelah tahap pengembangan sistem selesai dilakukan. Tujuannya ialah guna mengevaluasi sistem yang nantinya akan dihentikan, dilanjutkan ataupun dimodifikasi,
   - General Audit, Auditor menilai pengendalian atas pengembangan sistem secara keseluruhan. Auditor melakukan pendekatanini dengan tujuan untuk dapat mengurangi banyaknya substantive test yang dilakukan untuk menyatakan pendapat.

b. Evaluasi atas pengembangan sistem

   - Defenisi permasalahan, untuk memastikan apakah perusahaan *(stakeholders)* mengetahui apa resiko dan peluang yang mungkin terjadi terkait dengan penambahan suatu sistem informasi tersebut.

- Manajemen perubahan, dengan menitikberatkan pada mempersiapkan perubahan dalam perusahaan dengan pendekatan mendidik *unfreezing the organization)*; berubah ke sistem yang baru *(moving the organization)*; menolong siapa saja yang berkaiatan dengan sistem utnutk beradaptasi dan merasa nyaman dengan sistem yang baru ini *(refreezing the organization)*
- Studi kelayakan

Perlu dilakukan untuk memperoleh komitmen perubahan dari seluruh bagian yang bakal berubah dan mempelajarai secara *cost-effective* apakah perubahan ini bisa dilakukan atau tidak, dan memastkan tidak akan menimbulkan permasalahan dikemudian hari. Ada 4 studi kelayakan yang erlu dilakukan perusahaan yaitu : technical feasibiity, operational feasibility, economic feasibilty, behavioral feasibility.

- Analisa sistem yang ada

Jika sistem yang baru akan direkomendasikan untuk menggantikan sistem yang ada maka ada bebeapa hal yang perlu dilakukan perusahaan yaitu : mempelajari latar belakang, struktur dan budaya organisasi yang ada sekarang untuk mendapatkan pemahaman yang matang; mempelajari arus produk dan informasi yang akan diusulkan sis sietem yang baru.

- Menyusun kebutuhan strategis
- Mendesain organisasi dan pekerjaan
- Mendesain sistem pemrosesan informasi, dengan memeriksa enam aktifitas utama, yaitu :

1. Pendeskripsian kebutuhan strategis untuk meminimalisir ketidakpastian di sekeliling sistem
2. Memastikan bahwa hasil sistem ini memang benar-benar seperti yang diharapkan dan sesuai rencana
3. Mengevaluasi keputusan dalam ruang lingkup database untuk mendefenisikan hal tersebut akan dilaksanakan atau tidak
4. Memastikan pakah desainer sudah mengikuti suatu standar yang berhubungan dengan bagaimana membuat suatu desain yang baik
5. Menitikberatkan perhatian apakah gambaran fisik desain sudah cukup baik atau tidak
6. Memastikan agar desain yang dibuat bisa terintegrasi dengan baik dengan *hardware* atau *software* yang sudah ada.

- Akuisisi/Pengembangan aplikasi
- Akuisisi perangkat lunak
- Pengembangan prosedur
- Uji penerimaan
- Konversi dan implementasi
- Operasi dan pemeliharaan

2. Pemrograman

1. Karakteristik Pemrograman

Dalam melaksanakan evaluasi atas manajemen pemrograman auditor harus memahami dan memfokuskan perhatiannya pada beberapa karakteristik program yang berkualitas tinggi, yaitu :

- Berfungsi secara benar dan lengkap
- Mempunyai interface pengguna yang berkualitas tinggi
- Bekerja secara efektif
- Didesain dan didokumentasikan dengan baik
- Mudah dipelihara
- Tahan terhadap kondisi yang abnormal

Beberapa hal penting dalam pengendalian manajemen pemrograman adalah:

- Gunakan staf pemrograman yang berkualitas tinggi
- Sedapat mungkin lakukan pemisahan fungsi
- Kembangkan dan dokumentasikan metodologi dan standar kinerja
- Batasi kewenangan programer
- Pelihara log manual dan log komputer atas aktivitas program
- Gunakan konsultan luar untuk mengevaluasi pekerjaan pemrograman
- Lakukan penilaian silang atas kinerja programer secara periodik

2. Evaluasi atas manajemen pemrograman

- Tahap perencanaan, Dalam tahap perencanaan yang paling sulit dilakukan adalah perkiraan biaya pemrograman. Audit sebaiknya mengetahui beberapa teknik perkiraan biaya pemrograman.
- Tahap Desain, Jika suatu program akan dikembangkan atau dimodifikasi maka pasti akan ada fase desain. Dalam hal ini akan sangat banyak jenis pendekatan desain model, maka diharapkan seorang auditor mengetahui secara umum dan mengapa programmer umumnya menggunakan pendekatan itu.
- Tahap Coding, Selama tahap coding ini programmer melakukan penulisan progam yang pada akhirnya akan membuat program itu menjalankan perintah yang kita inginkan. Sejalan dengan semakin besarnya modul yang akan dibuat maka semakin banyak pula modul-modul di dalamnya.

- Tahap Testing, Tahap ini di tunjukkan untuk mengidentifikasikan adanya kesalahan, bukan ketidakberadaan kesalahan. Tahap-tahap umum yaitu : memilih batasan pengujian, menentukan sasaran pengujian, memilih pendekatan pengujian, mengembangkan pengujian, melakukan pengujian, mengevaluasi pengujian dan mendokumentasikan pengujian.
- Tahap operasi dan pemeliharaan, Beberapa aktifitas utama pada tahap ini yang perlu dievaluasi oleh auditor adalah monitoring kinerja dan jeni-jenis pemeliharaan dan perbaikan yang dilakukan serta pengendalian perangkat lunak manajemen konfigurasi yang digunakan.

3. Operasional

- Computer Operational Control. Terdiri dari : **operation control** (untuk menentukan apakah fungsi manusia atau operasi otomasi yang harus dilakukan); **schedulling control** (untuk memastikan ahwa sumber daya hardware yang dimiliki oleh perusahaan digunakan hanya oleh personil yang berhak dan hanya digunakan untuk kepentingan perusahaan saja; **maintenance control** (menentukan bagaimana perangkat keras harus dipelihara untuk mencegah kerusakan dan memfungsikan kembali hardware yang rusak.
- Network Operation Control. Terdiri dari LAN controls dan WAN Controls. LAN controls berhubungan dengan kegiatan di Local Area Network, dimana manajemen operasi dalam LAN terjadi melalui fasilitas-fasilitas yang diberikan oleh file server. Wan controls merupakan pengendalian jaringan dalam lingkungan yang lebih luas. Ada suatu keadaan dimana operator harus mengidentifkasi kejadian tertentu dan mengkonfigurasi ulang jaringan untuk mengatasi masalah. Alat yang biasanya berguna untuk jaringan bersar ini disebut Network Control Terminal (NCT) dimana hanya hanya operator senior yang terlatih baik yang akan melaksanakan pengendalian guna menjaga keamanan aset dan integritas data dalam NCT.
- Data Preparation dan Entry

Meliputi :

1. Source document design, dimana sebuah sumber dokumen terstruktur dengan baik, data apa saja yang dicatat, siapa yang mencatat, atau bagaimana dokumen tersebut disimpan ke dalam sistem.
2. Source document storage, dimana sumber yang telah dientry diberi tanda dan tidak boleh dientry kembali dan dikendalikan dengan baik penyimpananya

3. Inpput screen design, dimana perancangan tampilan layr input disesuaikan dengan dokumen sumber dan meperhatikan kemudahan pengguna dan kecepatan entry data.
4. Data entry area design, dimana desain area pemsukan data harus embuat nyaman operator.

- Production control. Meliputi receipt & dispatch of input &output, job schedulling, user service level agreement, transfer pricing or charge out control dan computer consumables.
- File library control. Bertanggung jawab terhadap pengorganisasian penggunaan media penyimpanan, seperti storage of storage media, use of storage media, maintenance and disposal of storage media, location of storage media.
- Documentation and program library control. Auditor dapat mengevalusi dengan menanyakan pada *documentation librarians* tetang tugas mereka, bagaiaman mereka mengorganisir penyimpanan dokumentasi danmemeriksa serta memastikan pencatatan dokumentasi berada dalam tempat yang aman sehingga orang yang tidak bertanggung jawab tidak bisa merubah dan memanfaatkan dokumentasi tersebut.
- Helpdesk/technical support control. Yang berfungsi : membantu end-user menggunakan hardware dan software, menyediakan dukungan y=teknis bagi sistem produksi dengan membantu memecahkan permasalahan.
- Mengevaluasi profil kinerja akan adanya aktifitas yang tidak terotorisasi. Auditor mengevaluasi bagaimana manajemen operasi menorganisir perencanaan kapasitas dan fungsi monitor performance. Akan lebih baik jika tersedia catatan statistik mengenai monitor pekerjaan mereka.
- Management of outsourced operations controls.

Ada 4 pengendalian jika suatu perusahaan akan melakukan outsourcing, yaitu :

1. Evaluasi atas kemampuan finansial vendor
2. Memastikan ketaatan terhadap termin dan kondisi kontrak
3. Memastikan kemampuan untuk mengendalikan operasi vendor
4. Menjaga disaster recovery planning

Nama : Moh Fajri Al Amin

Nim : 182420121

Kelas : MTI. 20A

DosenPengasuh : Dr Widya Cholil , S.Kom., M.I.T.

Mata Kuliah : IT Audit

Soal

untuk proses control (pengendalian) ada tindakan yang perlu dilaksanakan, gunakan referensi yang ada untuk menjawap pertanyaan saya tertutama dalam hal pengembangan sistem, pemrogramaan dan operasional.

Jawab:

Pengendalian internal adalah pengendalian dalam suatu organisasi bertujuan untuk menjaga aset perusahaan, pemenuhan terhadap kebijakan dan prosedur, kehandalan dalam proses, dan operasi yang efisien.

tujuan disusunnya system control atau pengendalian internal komputer adalah sebagai berikut:

Meningkatkan pengamanan (improve safeguard) aset sistem informasi (data/catatan akuntansi (accoun5ng records) yang bersifat logical assets, maupun physical assets seperA hardware, infrastructures, dan sebagainya).

Meningkatkan integritas data (improve data integrity), sehingga dengan data yang benar dan konsisten akan dapat dibuat laporan yang benar.

Meningkatkan efekAfitas sistem (improve system effec5veness).

Meningkatkan efisiensi sistem (improve system efficiency)

Pengembangan Sistem.

Pengembangan sistem bisa termasuk pembelian maupun in-house development atas sistem informasi sesuai dengan kebutuhan organisasi. Hal yang patut diperhatikan dalam pengembangan sistem adalah dibentuknya tim yang terdiri atas personel IT serta personel non IT dari kalangan pengguna. Hal ini memperbesar kemungkinan seluruh kebutuhan informasi, desain sistem, dan implementasi tersampaikan dengan baik. Melibatkan pengguna ke dalam proses pengembangan juga menyediakan hasil yang lebih baik dalam hal acceptance dari pihak pengguna.

Selain itu perlu pula dilaksanakan pengujian atas sistem informasi. Meliputi uji kerentanan (penetration-test) serta uji beban (stress-test). Dan yang tidak kalah pentingnya adalah pembuatan dokumentasi yang memadai atas sistem informasi yang dikembangkan, serta ditransfer kepada librarian.

Tiga area umumdalam audit yang berkaitan dengan proses pengembangan sistemadalah standar-standar pengembangan sistem, manajemen proyek, dan pengendalian pengubahan program.

Standar-standar pengembangan sistem, merupakan dokumentasi yang menjadi panduan perancangan, pengembangan, dan implementasi sistem aplikasi. Keberadaan standar-standar pengembangan sistem merupakan pengendalian umum utama dalam sistem audit.

Manajemen proyek, untuk mengukur dan mengendalikan perkembangan selama pengembangan sistem aplikasi. Manajemen proyek meliputi proyek dan penyeliaan proyek. Perencanaan proyekmerupakan pernyataan formal mengenai rencana-rencana kerja rinci dalam proyek. Penyeliaan proyek memonitor pelaksanaan aktifitas-aktifitas proyek.

Pengendalian pengubahan program, berkaitan dengan pemeliharaan program-program aplikasi. Tujuan pengendalian-pengendalian tersebut adalah untuk mencegah pengubahan yang tidak sah dan bersifat penggelapan terhadap program-program yang telah di uji dan di terima

Tujuan dari kontrol input adalah kebenaran, keakuratan dan kelengkapan input data. Dua penyebab umum dari kesalahan input:

· kesalahan transkripsi yaitu kesalahan pada karakter atau nilai

· kesalahan transposisi yaitu karakter atau nilai 'benar', tetapi di tempat yang salah

Ada beberapa contoh dalam kontrol input:

Ø Check digit- kode data yang ditambahkan untuk menghasilkan digit kontrol. angat berguna untuk transkripsi dan transposisi kesalahan

Ø Missing data checks - kontrol untuk pembenaran yang kosong atau yang salah

Ø Numeric-alphabetic checks- memverifikasi bahwa karakter dalam bentuk yang benar

Ø Limit checks - mengidentifikasi nilai-nilai di luar batas dari yang sebelumnya telah ditentukan

Ø Range checks- mengidentifikasi nilai-nilai luar batas atas dan bawah

Ø Reasonableness checks - membandingkan satu bidang ke bidang lainnya untuk melihat apakah hubungan sesuai

Ø Validity checks- membandingkan nilai ke nilai-nilai yang diketahui atau nilai standar

b. Pengendalian Aplikasi Pemrosesan

Proses diprogram untuk mengubah input data menjadi informasi untuk menghasilkan output. Ada Tiga kategori:

a. Batch controls, yaitu menyesuaikan sistem output dengan input awalnya yang dimasukkan ke dalam sistem. Berdasarkan jenis total batch:

· Total angka catatan

· Total nilai dolar

· Total campuran yaitu jumlah angka non-keuangan

b. Run-to- run controls, menggunakan angka batch untuk memonitor batch ketika bergerak dari satu prosedur program (run) ke yang lain.

c. Audit trail controls, banyak buku catatan yang digunakan sehingga setiap transaksi dapat ditelusuri melalui setiap tahapan pengolahan dari sumber ekonomi untuk presentasi dalam laporan keuangan. Contohnya adalah :

- Transaction logs, setiap transaksi dari sistem proses yang suskes akan dicatat pada buku harian, dimana tersaji seperti jurnal.

- Log of automatic transactions, sistem yang menggerakan beberapa transaksi internal.

- Transaction listings, sistem akan memproduksi daftar transaksi dari semua transaksi yang suskes.

c. Pengendalian Aplikasi Output

Tujuan dari kontrol output untuk memastikan bahwa sistem output tidak hilang, salah arah, atau rusak, dan privasi yang tidak dilanggar. Beberapa hal yang perlu dilakukan agar pengendalian output ini baik :

a. Output spooling, menciptakan sebuah file selama proses pencetakan yang mungkin tidak tepat diakses

b. Printing, membuat dua risiko:

· memproduksi salinan yang tidak sah dari output

· penjelajahan karyawan tentang data sensitif

c. Waste - dapat dicuri jika tidak dibuang dengan benar, misalnya, merobek-robek

d. Report distribution – untuk laporan sensitif, berikut yang bisa dilakukan:

· menggunakan kotak surat yang aman

· mengharuskan pengguna untuk mendaftar untuk laporan secara pribadi

· menyampaikan laporan kepada pengguna

e. end user controls - pengguna akhir harus memeriksa laporan sensitif untuk ketelitiannya

f. controlling digital output – pesan output digital dapat ditahan, digganggu, hancur, atau rusak karena melewati sepanjang link komunikasi.

Pemprograman.

Karakteristik Pemrograman

Dalam melaksanakan evaluasi atas manajemen pemrograman auditor harus memahami dan memfokuskan perhatiannya pada beberapa karakteristik program yang berkualitas tinggi, yaitu :

Berfungsi secara benar dan lengkap

Mempunyai interface pengguna yang berkualitas tinggi

Bekerja secara efektif

Didesain dan didokumentasikan dengan baik

Mudah dipelihara

Tahan terhadap kondisi yang abnormal

Beberapa hal penting dalam pengendalian manajemen pemrograman adalah:

Gunakan staf pemrograman yang berkualitas tinggi

Sedapat mungkin lakukan pemisahan fungsi

Kembangkan dan dokumentasikan metodologi dan standar kinerja

Batasi kewenangan programer

Pelihara log manual dan log komputer atas aktivitas program

Gunakan konsultan luar untuk mengevaluasi pekerjaan pemrograman

Lakukan penilaian silang atas kinerja programer secara periodik

Evaluasi atas manajemen pemrograman

Tahap perencanaan, Dalam tahap perencanaan yang paling sulit dilakukan adalah perkiraan biaya pemrograman. Audit sebaiknya mengetahui beberapa teknik perkiraan biaya pemrograman.

Tahap Desain, Jika suatu program akan dikembangkan atau dimodifikasi maka pasti akan ada fase desain. Dalam hal ini akan sangat banyak jenis pendekatan desain model, maka diharapkan seorang auditor mengetahui secara umum dan mengapa programmer umumnya menggunakan pendekatan itu.

Tahap Coding, Selama tahap coding ini programmer melakukan penulisan progam yang pada akhirnya akan membuat program itu menjalankan perintah yang kita inginkan. Sejalan dengan semakin besarnya modul yang akan dibuat maka semakin banyak pula modul-modul di dalamnya.

Tahap Testing, Tahap ini di tunjukkan untuk mengidentifikasikan adanya kesalahan, bukan ketidakberadaan kesalahan. Tahap-tahap umum yaitu : memilih batasan pengujian, menentukan sasaran pengujian, memilih pendekatan pengujian, mengembangkan pengujian, melakukan pengujian, mengevaluasi pengujian dan mendokumentasikan pengujian.

Tahap operasi dan pemeliharaan, Beberapa aktifitas utama pada tahap ini yang perlu dievaluasi oleh auditor adalah monitoring kinerja dan jeni-jenis pemeliharaan dan perbaikan yang dilakukan serta pengendalian perangkat lunak manajemen konfigurasi yang digunakan.

Operasional

Operation Control - Pengendalian ini menentukan apakah fungsi manusia atau operasi otomasi yang harus dilakukan. Banyak jenis aktivitas yang harus dilakukan untuk mendukung jalannya program di komputer,

contohnya : program-program harus dijalankan ataupun dihentikan, media penyimpanan harus di isi dengan data yang up-to-date, berbagai formulir dan dokumen harus di cetak di printer dan lain sebagainya.

Di jaman yang modern ini ada juga kemungkinan penggunaan automated operations facilities (AOFs) yang melakukan semua pekerjaan manual diatas secara otomatis. Campur tangan manusia akan menjadi semakin kecil jika sudah menggunakan AOFs ini.

Jenis – jenis operasi diatas tersebut adalah operasi normal dari komputer. Ketika semakin banyak operasi komputer dilakukan secara terotomatisasi, auditor harus menitikberatkan pemeriksaan pada masalah-masalah authentifikasi, akurasi, dan kelengkapan dari program yang berjalan terotomatisasi tersebut. Pertanyaan yang harus diyakinkan terjawab oleh auditor ialah:

Siapa yang bertanggungjawab atas desain, implementasi, dan pemeliharaan dari AOFs ini?

Apakah sewaktu mendesain, mengimplementasi, dan memelihara terdapat standar-standar tertentu yang dipatuhi?

Apakah AOFs dipelihara dalam lingkungan yang aman?

Seberapa seringkah AOFs yang baru atau yang hasil modifikasi di test?

Apakah saat ini terdapat proses monitoring yang berkelanjutan terhadap proses otentifikasi, akurasi dan kelengkapan dari operasi AOFs ini?

Seberapa baikkah lingkungan AOFs di dokumentasikan?

Apakah ada salinan dari dokumen lingkungan AOFs yang dibuat sebagai back-up dan dipisahkan di tempat yang lain?

Scheduling Control – Pengendalian ini yang menentukan bagaimana sebuah pekerjaan harus dijadwalkan dalam lingkungan platform perangkat keras dan lunak. Inti dari pengendalian ini ialah untuk memastikan bahwa sumber daya hardware yang dimiliki oleh perusahaan digunakan hanya oleh personil yang berhak dan juga hanya digunakan untuk kepentingan perusahaan semata. Bisa saja misalnya seorang personil yang tidak bertanggung jawab menggunakan hardware yang dipinjamkan oleh perusahaan untuk keperluannya pribadi. Salah satu cara untuk mencegah hal ini ialah dengan melakukan pemeriksaan terjadwal.

Seorang auditor sebaiknya memeriksa eksistensi dan skedul-skedul dari operasi perusahaan. Jika skedul itu belum ada atau kalaupun ada tidak selalu dipatuhi, maka titik berat pemeriksaaan akan difokuskan dalam bagaimana mengefektifkan dan mengefisienkan skedul tersebut. Kalau hal ini tidak dilakukan maka kemungkinan akan banyak pekerjaan-pekerjaan yang tidak selesai tepat waktu dan sumberdaya software tidak secara efisien digunakan. Dalam hal ini maka auditor harus melakukan substantive test untuk lebih memperjelas pemahaman sebagai contoh apakah user puas dengan sistem aplikasinya dan apakah berbagai jenis sumber daya mesin mempunyai tingkat daya guna yang tinggi.

Maintenance Control – Pengendalian ini yang menentukan bagaimana perangkat keras harus dipelihara. Pemeliharaan hardware komputer adalah merupakan tindakan untuk mencegah kerusakan, sedangkan Perbaikan adalah usaha untuk memfungsikan kembali hardware yang sudah lebih dahulu rusak.

Secara umum pemeliharaan akan berbanding terbalik dengan perbaikan. Semakin sering pemeriksaan maka akan semakin kecil kemungkinan kerusakan terjadi. Ada dua faktor yang mempengaruhi kebijakan pemeliharaan dan perbaikan harus dilakukan yaitu (1) lokasi dari hardware dan (2) tingkat pentingnya suatu hardware terhadap operasi perusahaan. Jika letak hardware jauh dari perusahaan (misalnya perusahaan tambang) dimana akses untuk petugas pemeliharaan relatif susah maka tindakan pemeliharaan akan semakin sering dilakukan.

Perhatian utama auditor dalam hal pemeliharaan hardware adalah efektifitas dan efisiensi. Jika hardware tidak dapat diandalkan, output yang diharapkan juga tidak akan sesuai dengan yang diharapkan. Penjagaan aset dan integritas data juga berisiko dalam hal ini, dimana hardware yang tidak baik kemungkinan akan merusakkan data. Data yang rusak pada gilirannya bisa menghilangkan kesempatan pengambilan keputusan yang baik.

Untuk memeriksa hal ini maka auditor dianjurkan untuk melakukan interview dengan manager operasi perusahaan, para insinyur, dan operator untuk mendapatkan gambaran yang jelas mengenai aktivitas apa saja yang sudah dilakukan dan bagaimana dilakukannya.

Network Operation Control

LAN Controls - Manajemen operasi inilah yang khusus berhubungan dengan kegiatan di Local Area Networks (LAN). Manajemen operasi dalam LAN terjadi melalui fasilitas-fasilitas yang diberikan oleh file server.

File server adalah sebuah komputer yang berada dalam LAN dan bertugas memberikan berbagai macam layanan seperti berbagi data dan program (misalnya database, spreadsheet, dll) dan juga otorisasi dan konfigurasi data.

File server merupakan komponen yang kritikal dalam LAN karena mereka menyimpan data dan program yang sensitif yang dapat di manfaatkan untuk melemahkan integritas dan keamanan jaringan. Contohnya ialah akses ke file server dapat membolehkan suatu alat yang tadinya tidak tersambung menjadi tersambung dan sebaliknya, dalam kasus ini file server sebaiknya berada dalam ruangan yang aman (physical barrier).

Dalam mengevaluasi hal ini auditor dapat melakukan interview, observasi, dan mereview dokumentasi-dokumentasi yang berhubungan dengan evaluasi reliabilitas alat kendali dalam LAN tersebut. Contohnya seorang auditor meng-interview seorang staf yang bertanggungjawab untuk mengoperasikan dan memperoleh keterangan yang lebih lanjut tentang bagaimana prosedur mereka dalam mengawasi sumberdaya software dan hardware yang tersambung ke LAN mereka. Auditor juga dapat melihat secara langsung apakah file server berada dalam lingkungan yang aman dan ada batasan siapa saja yang boleh masuk ke sana atau apakah banyaknya ruangan dalam media penyimpanan yang boleh dimanfaatkan terus dilaporkan tingkat penggunaannya.

WAN Controls - Pengendalian ini merupakan pengendalian jaringan dalam lingkungan yang lebih luas dari LAN. Dalam WAN, banyak tipe-tipe insiden yang membutuhkan campur tangan manusia terjadi, misalnya : jalur komunikasi kemungkinan terganggu, suatu program terputus secara tidak wajar, dan lain- lain.

Seorang operator yang baik harus bisa mengidentifikasi kejadian- kejadian seperti ini dan mengkonfigurasi ulang jaringan untuk mengatasi hal tersebut. Alat yang biasanya sangat berguna bagi operator jaringan besar ini dinamakan Network Control Terminal atau NCT.

Sebuah NCT bisa menyediakan akses ke software khusus yang membolehkan fungsi-gungsi dibawah ini berjalan:

Menjalankan dan menghentikan suatu proses,

Memonitor tingkat aktivitas jaringan,

Membuat statistik penggunaan sistem,

Merapikan daftar antrian program,

Meningkatkan frekuensi back-up,

Meng-inquiring status sistem yang berjalan,

Mengirimkan pesan peringatan dan pesan status, dan

Mengevaluasi data yang dipakai bersama dalam jalur komunikasi.

Dari sudut pandang pengamanan aset dan penjagaan integritas data sebuah NCT adalah alat yang sangat diperlukan. Penggunaan yang tidak pada tempatnya akan mengakibatkan kerugian yang besar pada jaringan perusahaan.

Seorang auditor dapat mengevaluasi bagian ini dengan memeriksa reliabilitas dari kebijakan-kebijakan yang sudah diterapkan oleh perusahaan untuk bagian ini. Evaluasinya dengan menggunakan interview, observasi, dan review dokumentasi bagian ini. Contohnya auditor dapat meng-interview operator jaringan untuk mengevaluasi apakah staf tersebut memiliki kompetensi yang cukup untuk mengemban tanggungjawab tersebut.

Data Preparation & Entry

Secara umum semua sumber data bagi sistem-sistem aplikasi bisa diperoleh dari file atau dengan memsukkan ke dalam aplikasi tersebut. Sudah banyak kita lihat di mal-mal dimana kasir (terminal point of sales) menggunakan key outomatic reader dengan membaca bar code dari barang yang memang sudah tersimpan dalam database aplikasi tersebut. Kalau sedang bermasalah apakah karena barangnya rusak atau basah sehingga bar code tidak bisa dibaca, maka kasir akan memasukkan datanya secara manual melalui tombol-tombol di cash register. Dalam membuat aplikasi tersebut tidak sembarangan dibuat karena ada kaedah-kaedahnya. Kalau aturan itu tidak dipatuhi maka akan ada resiko yang dialami oleh perusahaan dalam hal ini mungkin kasir di cash register yang lelah karena terlalu lama dalam menyelesaikan tugas-tugasnya akibat dokumen yang tidak ter-design dengan baik.

Source Document Design - Dari sudut pandang pengendalian sebuah sumber dokumen yang terstruktur dengan baik akan menjelaskan data apa yang akan dicatat, bagaimana data tersebut akan dicatat, siapa yang akan mencatat data tersebut dan memasukkannya ke dalam komputer dan bagaimana dokumen disimpan dan difilekan.

Source Document Storage – Dokumen-dokumen sumber yang telah dientri ke dalam sistem sebaiknya diberi tanda bahwa telah dientri dan tidak boleh digunakan/dientri kembali serta dikendalikan dengan baik penyimpanannya.

Input Screen Design – Perancangan tampilan layar untuk melakukan entri data sebaiknya disesuaikan dengan dokumen sumber serta memperhatikan kemudahan penggunaan dan kecepatan entri data.

Data Entry Area Design - Desain area pemasukan data akan mempengaruhi kenyamanan operator, antara lain :

Area penyinaran di cukup dan tidak berlebihan yang menyebabkan silau.

Lingkungan kerja sebaiknya senyaman mungkin, tidak terlalu berisik dan tidak terlalu sunyi.

Desain ruangan kerja tidak berantakan untuk memudahkan melakukan aktivitas kerja.

Perabotan di desain sedemikian rupa agar bisa meminimalisir cedera ringan yang mungkin terjadi.

Resiko yang akan terjadi jika hal-hal diatas tidak ditangani dengan baik antara lain adalah Repetition Stain Injury (RSI) & Occupational Overuse Syndrome (OSS) diestimasikan mencapai

$50 Milyard per tahunnya (Australian Financial Review, 4 Maret 1992)

Sumber :

http://yulhendri.weblog.esaunggul.ac.id/wp-content/uploads/sites/5361/2015/12/Audit-SI_TI.pdf

https://mihok.my.id/pengendalian-internal-berkaitan-dengan-it/

NAMA : MOH. RENDY SEPTIYAN

NIM : 182420103

MATA KULIAH : IT AUDIT

Control dan Audit IT

Referensi 1 ***(Sumber :*** http://asihcahyani28.blogspot.com/2016/11/dua-pengendalian-it-two-it-controls.html)

Pengendalian IT itu ada dua, yaitu ada yang terkait secara langsung dengan transaksi dan ada juga yang tidak terkait langsung dengan transaksi. Pengendalian yang terkait secara langsung dengan transaksi disebut dengan pengendalian aplikasi (Application Control), sedangkan yang tidak terkait langsung dengan transaksi disebut dengan pengendalian umum (General Control).

A. Pengendalian Umum (General Controls)

Pengendalian umum adalah kebijakan dan prosedur yang berhubungan dengan aplikasi sistem informasi dan mendukung fungsi dari application control dengan cara membantu menjamin keberlangsungan sistem informasi yang ada. Tujuannya adalah untuk menjamin keamanan dan stabilitas sistem secara keseluruhan. Pengendalian ini berhubungan dengan luasnya cakupan entitas yang terkomputerisasi, serta berlaku untuk semua sistem dan mengatur pemerintahan dan infrastruktur, keamanan sistem operasi dan database, dan aplikasi dan program akuisisi dan pembangunan IT. Contohnya adalah kontrol atas pusat data, database organisasi, pengembangan sistem, dan pemeliharaan program. Pengendalian umum pada perusahaan biasanya dilakukan terhadap aspek fisikal maupun logikal. Aspek fisikal, terhadap aset-aset fisik perusahaan, sedangkan aspek logikal biasanya terhadap sistem informasi di level manajemen (misal: sistem operasi). Pengendalian umum sendiri digolongkan menjadi beberapa, diantaranya adalah:

1. Pengendalian organisasi dan otorisasi.

Yang dimaksud dengan organisasi disini adalah secara umum terdapat pemisahan tugas dan jabatan antara pengguna sistem (operasi) dan administrator sistem (operasi). Disini juga dapat dilihat bahwa pengguna hanya dapat mengakses sistem apabila memang telah diotorisasi oleh administrator.

2. Pengendalian operasi.

Operasi sistem informasi dalam perusahaan juga perlu pengendalian untuk memastikan sistem informasi tersebut dapat beroperasi dengan baik selayaknya sesuai yang diharapkan.

3. Pengendalian perubahan.

Perubahan-perubahan yang dilakukan terhadap sistem informasi juga harus dikendalikan. Termasuk pengendalian versi dari sistem informasi tersebut, catatan perubahan versi,serta manajemen perubahan atas diimplementasikannya sebuah sistem informasi.

4. Pengendalian akses fisikal dan logikal.

Pengendalian akses fisikal berkaitan dengan akses secara fisik terhadap fasilitas-fasilitas sistem informasi suatu perusahaan, sedangkan akses logikal berkaitan dengan pengelolaan akses terhadap sistem operasi sistem tersebut (misal: windows).

B. Pengendalian Aplikasi (Application Controls)

Bertujuan untuk menjamin keandalan input, file, program dan output. Pengendalian ini memastikan integritas sistem tertentu. Berlaku untuk aplikasi dan program-program tertentu, dan memastikan kebenaran data, kelengkapan dan akurasinya. Contoh: kontrol atas pemrosesan pesanan penjualan, hutang, dan aplikasi penggajian.

Aplikasi ini memiliki risiko dalam aplikasi tertentu dan dapat mempengaruhi prosedur manual (misalnya: memasukkan data) atau tertanam prosedur (otomatis). Pengendalian aplikasi terdiri dari 3 kategori :

a. Kontrol Input
b. Kontrol Proses
c. Kontrol Output

a. Pengendalian Aplikasi Input

Tujuan dari kontrol input adalah kebenaran, keakuratan dan kelengkapan input data. Dua penyebab umum dari kesalahan input:

· kesalahan transkripsi yaitu kesalahan pada karakter atau nilai
· kesalahan transposisi yaitu karakter atau nilai 'benar', tetapi di tempat yang salah

Ada beberapa contoh dalam kontrol input:

Ø Check digit- kode data yang ditambahkan untuk menghasilkan digit kontrol. angat berguna untuk transkripsi dan transposisi kesalahan

Ø Missing data checks - kontrol untuk pembenaran yang kosong atau yang salah

Ø Numeric-alphabetic checks- memverifikasi bahwa karakter dalam bentuk yang benar

Ø Limit checks - mengidentifikasi nilai-nilai di luar batas dari yang sebelumnya telah ditentukan

Ø Range checks- mengidentifikasi nilai-nilai luar batas atas dan bawah

Ø Reasonableness checks - membandingkan satu bidang ke bidang lainnya untuk melihat apakah hubungan sesuai

Ø Validity checks- membandingkan nilai ke nilai-nilai yang diketahui atau nilai standar

b. Pengendalian Aplikasi Pemrosesan

Proses diprogram untuk mengubah input data menjadi informasi untuk menghasilkan output. Ada Tiga kategori:

a. Batch controls, yaitu menyesuaikan sistem output dengan input awalnya yang dimasukkan ke dalam sistem. Berdasarkan jenis total batch:

· Total angka catatan

· Total nilai dolar

· Total campuran yaitu jumlah angka non-keuangan

b. Run-to- run controls, menggunakan angka batch untuk memonitor batch ketika bergerak dari satu prosedur program (run) ke yang lain.

c. Audit trail controls, banyak buku catatan yang digunakan sehingga setiap transaksi dapat ditelusuri melalui setiap tahapan pengolahan dari sumber ekonomi untuk presentasi dalam laporan keuangan. Contohnya adalah :

- Transaction logs, setiap transaksi dari sistem proses yang suskes akan dicatat pada buku harian, dimana tersaji seperti jurnal.
- Log of automatic transactions, sistem yang menggerakan beberapa transaksi internal.
- Transaction listings, sistem akan memproduksi daftar transaksi dari semua transaksi yang suskes.

c. Pengendalian Aplikasi Output

Tujuan dari kontrol output untuk memastikan bahwa sistem output tidak hilang, salah arah, atau rusak, dan privasi yang tidak dilanggar. Beberapa hal yang perlu dilakukan agar pengendalian output ini baik :

a. Output spooling, menciptakan sebuah file selama proses pencetakan yang mungkin tidak tepat diakses

b. Printing, membuat dua risiko:

· memproduksi salinan yang tidak sah dari output

· penjelajahan karyawan tentang data sensitif

c. Waste - dapat dicuri jika tidak dibuang dengan benar, misalnya, merobek-robek

d. Report distribution – untuk laporan sensitif, berikut yang bisa dilakukan:

- menggunakan kotak surat yang aman
- mengharuskan pengguna untuk mendaftar untuk laporan secara pribadi
- menyampaikan laporan kepada pengguna

e. end user controls - pengguna akhir harus memeriksa laporan sensitif untuk ketelitiannya

Referensi 2 ***(Sumber :*** *https://it.proxsisgroup.com/bagaimana-audit-ti-dilakukan-bagian-1/*)

Pada dasarnya, Audit TI dapat dibedakan menjadi dua kategori, yaitu Pengendalian Aplikasi (*Application Control*) dan Pengendalian Umum (*General Control*). Tujuan pengendalian umum lebih menjamin integritas data yang terdapat di dalam sistem komputer dan sekaligus meyakinkan integritas program atau aplikasi yang digunakan untuk melakukan pemrosesan data. Sementara, tujuan pengendalian aplikasi dimaksudkan untuk memastikan bahwa data di-input secara benar ke dalam aplikasi, diproses secara benar, dan terdapat pengendalian yang memadai atas output yang dihasilkan.

Dalam audit terhadap aplikasi, biasanya, pemeriksaan atas pengendalian umum juga dilakukan mengingat pengendalian umum memiliki kontribusi terhadap efektifitas atas pengendalian-pengendalian aplikasi.

Dalam praktiknya, tahapan-tahapan dalam audit TI tidak berbeda dengan audit pada umumnya. Tahapan perencanaan, sebagai suatu pendahuluan, mutlak perlu dilakukan agar auditor mengenal benar objek yang akan diperiksa. Di samping, tentunya, auditor dapat memastikan bahwa *qualified resources* sudah dimiliki, dalam hal ini aspek SDM yang berpengalaman dan juga referensi praktik-praktik terbaik (*best practices*). Tahapan perencanaan ini akan menghasilkan suatu program audit yang didesain sedemikian rupa, sehingga pelaksanaannya akan berjalan efektif dan efisien, dan dilakukan oleh orang-orang yang kompeten, serta dapat diselesaikan dalam waktu sesuai yang disepakati.

Dalam pelaksanaannya, auditor TI mengumpulkan bukti-bukti yang memadai melalui berbagai teknik termasuk survei, interview, observasi dan review dokumentasi (termasuk review*source-code* bila diperlukan).

Satu hal yang unik, bukti-bukti audit yang diambil oleh auditor biasanya mencakup pula bukti elektronis (data dalam bentuk file softcopy). Biasanya, auditor TI menerapkan teknik audit berbantuan komputer, disebut juga dengan CAAT (*Computer Aided Auditing Technique*). Teknik ini digunakan untuk menganalisa data, misalnya saja data transaksi penjualan, pembelian, transaksi aktivitas persediaan, aktivitas nasabah, dan lain-lain.

Sesuai dengan standar auditing ISACA (*Information Systems Audit and Control Association)*, selain melakukan pekerjaan lapangan, auditor juga harus menyusun laporan yang mencakup tujuan

pemeriksaan, sifat dan kedalaman pemeriksaan yang dilakukan. Laporan ini juga harus menyebutkan organisasi yang diperiksa, pihak pengguna laporan yang dituju dan batasan-batasan distribusi laporan. Laporan juga harus memasukkan temuan, kesimpulan, rekomendasi sebagaimana layaknya laporan audit pada umumnya.

Studi Kasus

Sebuah Bank Swasta terkemuka menunjuk tim audit TI Ernst & Young untuk melakukan review atas penerapan sistem Perbankan yang terintegrasi. Pemeriksaan ini terbagi dalam dua fase. Pada fase pertama mencakup kegiatan, sebagai berikut:

1. Manajemen Proyek

Melakukan review atas manajemen proyek untuk memastikan bahwa semua outcome yang diharapkan tertuang dalam rencana proyek. Pada tahapan ini, auditor TI melakukan review atas project charter, sumber daya yang akan digunakan, alokasi penugasan dan analisa tahapan pekerjaan proyek.

2. Desain Proses dan Pengendalian Kontrol Aplikasi

Review mengenai desain pengendalian dalam modul-modul Perbankan tersebut, yaitu pinjaman dan tabungan. Untuk itu dilakukan review atas desain proses dimana auditor mengevaluasi proses, risiko dan pengendalian mulai dari tahapan input, proses maupun output.

3. Desain Infrastruktur

Review ini mencakup analisa efektivitas dan efisiensi desain infrastruktur pendukung (server, workstation, sistem operasi, database dan komunikasi data).

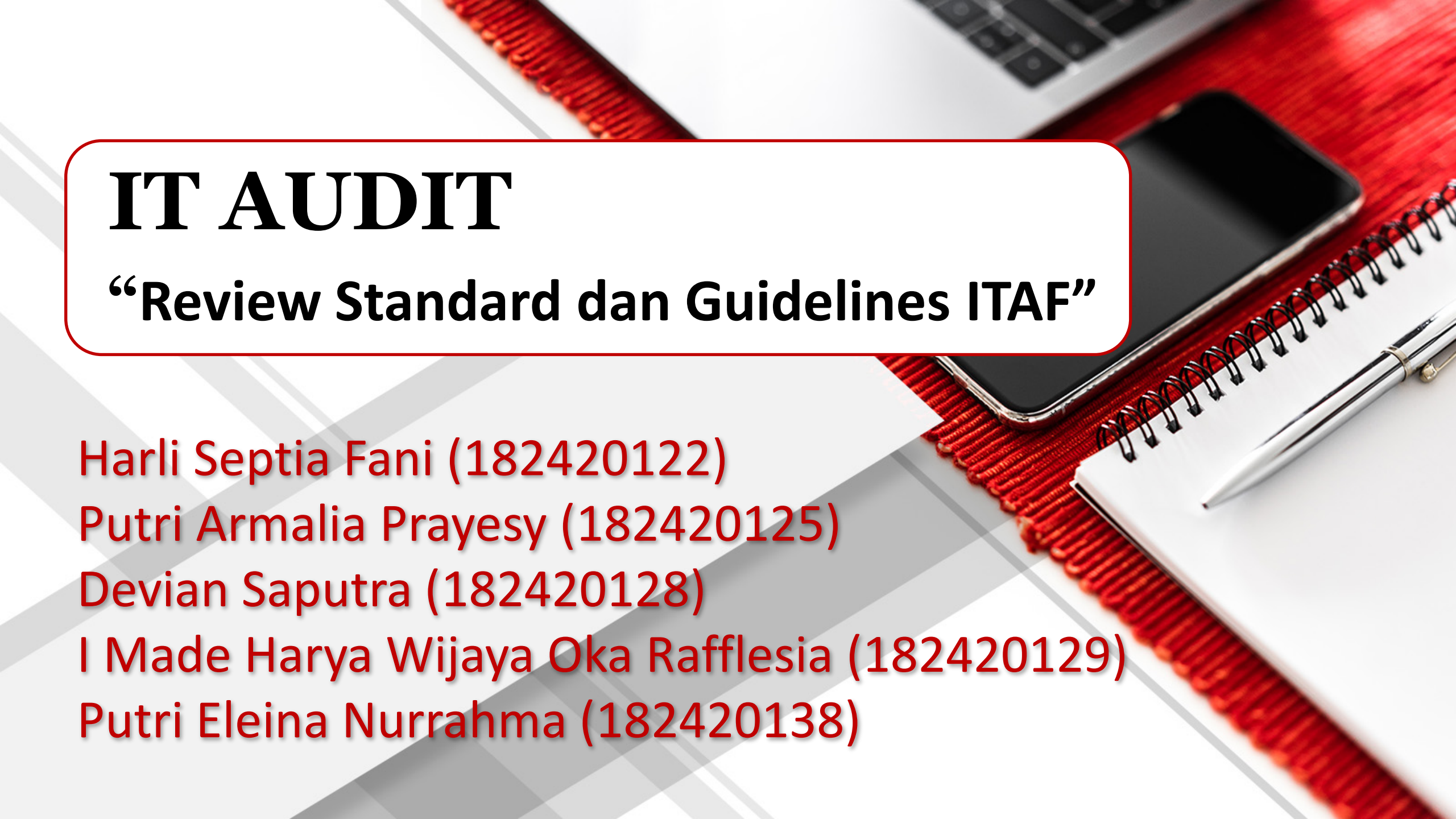
Hasil follow up dijadikan dasar oleh manajemen untuk memulai implementasi sistem Perbankan yang terintegrasi tersebut.

Berdasarkan nilai tambah yang diberikan melalui rekomendasi pada fase pertama, perusahaan menunjuk kembali auditor untuk melakukan review fase kedua secara paralel pada saat implementasi dilakukan, yaitu review terhadap:

- Migrasi data, pada saat “roll-out” ke cabang-cabang, termasuk kapasitas pemrosesan dan penyimpanannya.
- Aspek lainnya termasuk persiapan *help-desk* , *contingency* dan *security* .
- Kesiapan pemakai dalam menggunakan sistem ini, kualitas pelatihan yang diberikan dan dokumentasi pengguna (*user manual*)

- Prosedur-prosedur manajemen perubahan (*change management*) dan testing

Auditor selanjutnya diminta memberikan saran mengenai risiko-risiko yang masih tersisa, sebelum manajemen memutuskan sistem barunya dapat “go-live”.



IT AUDIT

"Review Standard dan Guidelines ITAF"

Harli Septia Fani (182420122)
Putri Armalia Prayesy (182420125)
Devian Saputra (182420128)
I Made Harya Wijaya Oka Rafflesia (182420129)
Putri Eleina Nurrahma (182420138)

1002 Independensi Organisasional

IS audit dan fungsi penjaminan adalah independensi dari area atau aktivitas yang sedang dilakukan untuk memungkinkan penyelesaian audit objektif dan jaminan perjanjian.

Tugas IS audit dan penjaminan :

- Melaporkan ke dalam tingkat organisasi yang diaudit yang menyediakan independensi organisasi dan memungkinkan audit dan jaminan fungsi untuk melakukan tanggung jawab tanpa gangguan
- Mengungkapkan rincian penurunan nilai untuk dilakukan kepada pihak-pihak yang tepat jika independensi terganggu dalam fakta atau penampilan
- Menghindari peran tanpa mengaudit dalam inisiatif yang membutuhkan asumsi tanggung jawab manajemen karena peran tersebut dapat merusak independensi yang akan datang
- Alamat independensi dan akuntabilitas fungsi audit dalam piagam atau surat perjanjian

Istilah

- Impairment
- Independensi
- Independensi dalam Penampilan
- Independensi dalam pemikiran
- Objektivitas

2002 Organisational Independence

Tujuannya adalah untuk mengatasi independensi fungsi audit dan jaminan IS di perusahaan.

Tiga Aspek penting :

- Kedudukan IS audit dan fungsi jaminan di dalam perusahaan;
- Tingkat dimana IS audit dan fungsi jaminan yang dilaporkan ke dalam perusahaan;
- Kinerja layanan non-audit dalam perusahaan oleh IS audit dan manajemen jaminan dan audit IS dan jaminan profesional.

• Kedudukan dalam Perusahaan

Untuk mengaktifkan organisasi yang mandiri, fungsi audit memerlukan kedudukan di dalam perusahaan yang mengizinkannya melaksanakan tanggung jawab tanpa campur tangan. Ini dapat dicapai degan :

- Membangun fungsi audit di dalam anggaran dasar audit sebagai fungsi independen atau departemen, di luar departemen operasional. Fungsi audit seharusnya tidak ditetapkan oleh aktivitas atau tanggung jawab operasional;
- Memastikan bahwa fungsi audit melaporkan ketingkat lebih tinggi di dalam perusahaan yang mengizinkan hal itu untuk mencapai kemandirian organisasi. Melaporkan kepimpinan departemen operasional dapat merundingkan kemandirian organisasi.

Fungsi audit harus mengabaikan peran non-audit dalam IS inisiatif yang memerlukan asumsi tanggung jawab manajemen, karena sebagian peran dapat mengganggu kemandirian dimasa depan. Kemandirian dan akuntabilitas fungsi audit harus diatasi dalam anggaran dasar audit.

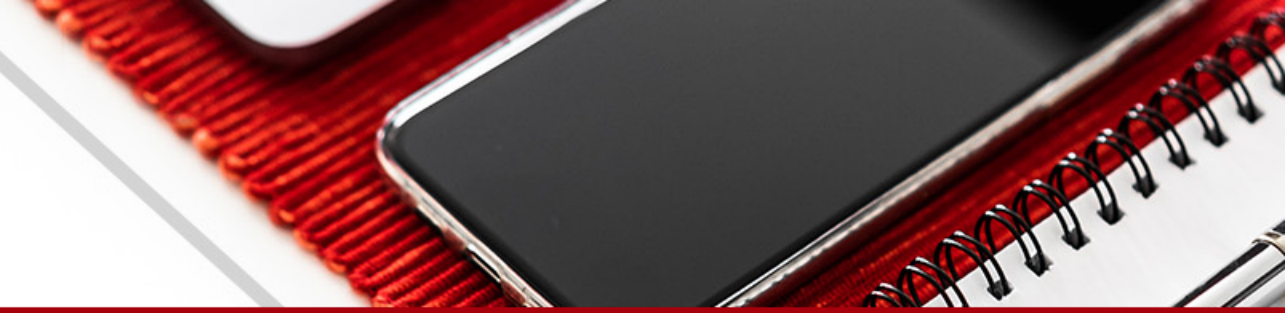
• Tingkat Laporan

Fungsi audit harus melaporkan ke suatu tingkat dalam organisasi yang mengizinkannya untuk bertindak dengan kemandirian organisasi yang lengkap. Kemandirian seharusnya didefenisikan dalam anggaran dasar audit dan dikonfirmasi oleh fungsi audit kepada Direksi dan yang dituntut dengan tata kelola secara teratur setidaknya setiap tahun.

Berikut yang harus dilaporkan oleh fungsi audit :

- Audit rencana sumber daya dan pengeluaran;
- Rencana audit (dengan berbasis resiko);
- Kinerja tindak lanjut yang dilakukan oleh fungsi audit pada aktifitas audit IS;
- Tindak lanjut cakupan yang signifikan atau keterbatasan sumber daya.

Untuk memastikan kemandirian organisasi dari fungsi audit, dukungan ekplisit diperlukan baik dari Manajemen dan dewan eksekutif.

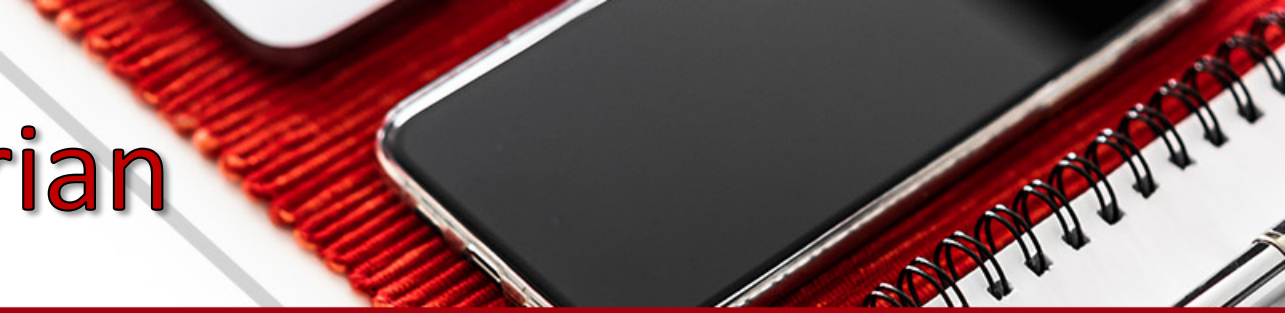


• Layanan non-Audit

Layanan non-audit berikut dianggap mengganggu kemandirian dan objektifitas, karena ancaman yang dibuat bisa sangat signifikan sehingga tidak ada pengamanan yang dapat menguranginya ketingkat yang dapat diterima :

- Dengan asumsi tanggung jawab manajemen atau melakukan kegiatan manajemen;
- Keterlibatan materi profesioanal dalam pengawasan atau kinerja perancangan, pengembangan, pengujian, pemasangan, konfigurasi atau mengoperasikan system informasi yang mana material atau signifikan terhadap pokok bahasan audit atau jaminan keterlibatan;
- Pengawasan perancangan untuk system informasi yang mana material atau pokokbahasan yang signifikan dari keterlibatan audit saat ini atau perencanaan dimasa depan;
- Melayani dalam peran tata kelola dimana para professional bertanggung jawab baik secara independen maupun secara bersama membuat keputusan manajemen atau menyetujui standar dan kebijakan;
- Memberikan saran yang merupakan dasar utama dari keputusan manajemen.

• Penilaian Kemandirian



Kemandirian harus dinilai secara berkala oleh fungsi audit dan secara profesional. Penilaian ini terjadi setiap tahun untuk fungsi audit dan sebelum setiap ikatan untuk para audit profesional. Penilaian harus mempertimbangkan faktor-faktor yang ada didalam nya seperti:

- Perubahan dalam hubungan pribadi
- Kepentingan finansial
- Penugasan dan tanggung jawab pekerjaan sebelumnya.

Anggaran dan Rencana Audit

- Anggaran audit harus merinci, di bawah aspek 'tanggung jawab', implementasi organisasi independensi fungsi audit. Selain merinci independensi, anggaran audit juga harus mencakup kemungkinan penurunan independensi.
- Independensi organisasi juga harus tercermin dalam rencana audit. Fungsi audit harus mampu menentukan ruang lingkup rencana secara mandiri, tanpa batasan yang diberlakukan oleh eksekutif pengelolaan.

Keterkaitan dengan Standar dan Proses COBIT 5

COBIT 5 Process	Process Purpose
EDM01 Pastikan pemerintahan mengatur kerangka kerja dan pemeliharaan.	Memberikan pendekatan konsisten yang terintegrasi dan selaras dengan tata kelola perusahaan pendekatan. Untuk memastikan bahwa keputusan terkait TI dibuat sejalan dengan perusahaan strategi dan tujuan, memastikan bahwa proses yang berhubungan dengan IT diawasi secara efektif dan secara transparan, kepatuhan terhadap persyaratan hukum dan peraturan dikonfirmasi, dan persyaratan tata kelola untuk anggota dewan dipenuhi.
APO01 Kelola kerangka Manajemen TI.	Memberikan pendekatan manajemen yang konsisten untuk memungkinkan tata kelola perusahaan persyaratan yang harus dipenuhi, meliputi proses manajemen, struktur organisasi, peran dan tanggung jawab, kegiatan yang dapat diandalkan dan berulang, dan keterampilan dan kompetensi.
MEA02 Monitor, mengevaluasi dan menilai sistem internal kontrol.	Transparansi bagi pelaku kepentingan utama tentang kecukupan sistem kontrol internal dan dengan demikian memberikan kepercayaan dalam operasi, kepercayaan dalam pencapaian tujuan perusahaan dan pemahaman yang memadai tentang risiko residual.

Istilah

- Independence (kemandirian) adalah kebebasan dari kondisi yang mengancam objektivitas atau penampilan objektivitas. Seperti itu ancaman terhadap objektivitas harus dikelola pada auditor individu, keterlibatan, fungsional dan organisasi. Dalam individu mencakup independensi pikiran dan kemandirian dalam penampilan.
- Objectivity adalah kemampuan untuk melakukan penilaian, mengekspresikan pendapat dan memberikan rekomendasi dengan keadilan.

Terima Kasih ☺

PROSES CONTROL YANG PERLUDILAKUKAN DALAM HAL PENGEMBANGAN SISTEM,PEMROGRAMAN,DAN OPERASIONAL

Proses control pengembangan system

Yang harus dilakukan dalam proses pengembangan system yang harus dilakukan terlebih dahulu memilih pendekatan yang sesuai dengan pengembangan system,pendekatan yang sangat cocok untuk proses control adalah pendekatan general audit yaitu auditor menilai atas pengembangan system secara keseluruhan dengan tujuan mengurangi substantive test yang diperlukan untuk menyatakan pendapat.

Manajemen Perubahan - Manajemen perubahan berjalan bersamaan dengan semua proses dalam pengembangan sistem. Ada tiga (3) aktivitas yang perlu dilakukan perusahaan selama perubahan ini yaitu :

- Unfreezing the organization - yaitu mempersiapkan perubahan dalam perusahaan dengan pendekatan mendidik.
- Moving the organization - yaitu berubah ke sistem yang baru dibuat.
- Refreezing the organization - yaitu menolong siapa saja yang berkaitan dengan sistem ini untuk beradaptasi dan merasa nyaman dengan sistem yang baru ini.

Studi kelayakan - Tujuan dari bagian ini ialah untuk memperoleh komitmen perubahan dari seluruh bagian yang bakal berubah dan mempelajari secara cost-effective apakah perubahan ini masih bisa dilakukan atau tidak. Ada empat (4) studi kelayakan yang perlu dilakukan oleh perusahaan yaitu:

- Technical Feasibility - Apakah tehnologi yang ada saat ini sanggup menjalankan sistem yang akan dibuat? dapatkah tehnologi tersebut dibuat dan dilaksanakan?
- Operational Feasibility - Apakah data yang dimasukkan ke sistem dapat dikumpulkan oleh sistem? Apakah hasilnya keluarannya dapat berguna?
- Economic Feasibility - Apakah biaya pembuatan sistem ini nantinya akan lebih kecil dari manfaat yang akan didapatkan dari sistem ini nantinya?
- Behavioral Feasibility - Dampak apa sajakah yang akan terjadi pada pengguna?

Analisa Sistem Yang Ada - Apabila sistem yang baru akan di rekomendasikan untuk menggantikan sistem yang ada. Desainer dari sistem perlu mengetahui sistem yang sudah ada. Ada beberapa hal yang perlu dilakukan oleh perusahaan yaitu:

- Mempelajari latar belakang struktur dan budaya organisasi, desainer perlu mempelajari sejarah perusahaan yang sekarang, struktur dan kebudayaan untuk memperoleh pemahaman yang prima. Auditor dalam hal ini menitikberatkan perhatian pada evaluasi keputusan desainer dalam hal (1) apakah mereka perlu mempelajari latar belakang perusahaan; (2) jika ya aspek apa yang perlu dipelajari; dan (3) tingkat kedalaman pemahaman yang perlu dipelajari.
- Mempelajari arus produk dan informasi, hal ini penting untuk tiga hal yaitu (1) kadangkala desain dari sistem yang akan diusulkan akan bertumpu pada produk

dan aliran informasi sistem yang ada sekarang. (2) desainer perlu mengerti kekuatan dan kelemahan dari produk yang ada. (3) pemahaman yang baik tentang produk yang ada dan aliran informasi akan diperlukan dalam proses implementasi sistem baru. Dalam hal ini auditor akan menitikberatkan perhatian pada tiga hal yaitu (1) harus dievaluasi setiap tanggapan atau reaksi dari stakeholders terhadap setiap usulan sistem, (2) auditor harus memeriksa apakah stakeholders menggunakan metode yang baik dalam menanggapi usulan sistem yang ajukan seperti object oriented analysis, dll. (3) auditor harus memastikan apakah desainer menggunakan alat perancangan yang baik seperti CASE (computer-aided software-engineering) tools untuk mendukung usulan mereka.

Menyusun Kebutuhan Strategis - Kebutuhan strategik yang perlu di penuhi oleh sistem ialah tujuan dari sistem yang kongkrit. Seperti mengurangi tingkat perputaran staf dalam area penjualan sebesar 30 %.

Mendesain Organisasi dan Pekerjaan - Dalam beberapa kasus, untuk mencapai kebutuhan strategis diperlukan desain atau desain ulang dari struktur organisasi dan pekerjaan

Proses control dalam manajemen program

Pengendalian atas manajemen pemrograman dapat dilakukan dengan memonitoring tahapan-tahapan yang ditempuh dibandingkan dengan rencana untuk memastikan efisiensi dan ketepatan waktu serta menilai pengendalian yang ada untuk memastikan autentikasi, akurasi dan kelengkapan. Monitoring dapat dilakukan menggunakan work breakdown structure, Gantt charts dan Program Evaluation & Review Techniques (PERT).

Beberapa hal penting dalam pengendalian manajemen pemrograman antara lain adalah :

- Gunakan staf pemrograman yang berkualitas tinggi
- Sedapat mungkin lakukan pemisahan fungsi
- Kembangkan dan dokumentasikan metodologi dan standar kinerja
- Batasi kewenangan programer
- Pelihara log manual dan log komputer atas aktivitas programer
- Gunakan konsultan luar untuk mengevaluasi pekerjaan pemrograman
- Lakukan penilaian silang atas kinerja programer secara periodik

Proses control dalam manajemen operasional

Pengendalian ini menentukan apakah fungsi manusia atau operasi otomasi yang harus dilakukan. Banyak jenis aktivitas yang harus dilakukan untuk mendukung jalannya program di komputer, contohnya : program-program harus dijalankan ataupun dihentikan, media penyimpanan harus di isi dengan data yang up-to-date, berbagai formulir dan dokumen harus

di cetak di printer dan lain sebagainya.

Adapun proses control pada manajemen operasional adalah sebagai berikut:

1. Scheduling Control – Pengendalian ini yang menentukan bagaimana sebuah pekerjaan harus dijadwalkan dalam lingkungan platform perangkat keras dan lunak. Inti dari pengendalian ini ialah untuk memastikan bahwa sumber daya hardware yang dimiliki oleh perusahaan digunakan hanya oleh personil yang berhak dan juga hanya digunakan untuk kepentingan perusahaan semata. Bisa saja misalnya seorang personil yang tidak bertanggung jawab menggunakan hardware yang dipinjamkan oleh perusahaan untuk keperluannya pribadi. Salah satu cara untuk mencegah hal ini ialah dengan melakukan pemeriksaan terjadwal.

2. Maintenance Control – Pengendalian ini yang menentukan bagaimana perangkat keras harus dipelihara. Pemeliharaan hardware komputer adalah merupakan tindakan untuk mencegah kerusakan, sedangkan Perbaikan adalah usaha untuk memfungsikan kembali hardware yang sudah lebih dahulu rusak.

3. LAN Controls - Manajemen operasi inilah yang khusus berhubungan dengan kegiatan di Local Area Networks (LAN). Manajemen operasi dalam LAN terjadi melalui fasilitas-fasilitas yang diberikan oleh file server.

4. WAN Controls - Pengendalian ini merupakan pengendalian jaringan dalam lingkungan yang lebih luas dari LAN. Dalam WAN, banyak tipe-tipe insiden yang membutuhkan campur tangan manusia terjadi, misalnya : jalur komunikasi kemungkinan terganggu, suatu program terputus secara tidak wajar, dan lain- lain.

5. File Library Control-Fungsi dari File Library dalam operasi ialah bertanggung jawab terhadap pengorganisasian penggunaan media penyimpanan.

6. Documentation & Program Library Control- Tugas utama documentation librarians adalah bertanggung jawab terhadap pengorganisasian dokumentasi ini yang termasuk didalamnya ialah: memastikan dokumentasi-dokumentasi tersebut berada dalam tempat yang aman, memastikan hanya personil yang berhak saja yang mendapat akses ke sana, memastikan bahwa isi dokumentasi itu up to date, memastikan ada back up yang cukup terhadap dokumentasi tersebut.

7. Help Desk/Technical Support Control Fungsi dari Help desk/technical support dalam organisasi ialah: membantu end-user menggunakan hardware dan software seperti aplikasi database, spreadsheet, dll. menyediakan dukungan tehnis bagi sistem produksi

8. Capacity Planning and Performance Monitoring Control Ditujukan untuk mengevaluasi apakah profil kinerja menunjukkan adanya aktivitas yang tidak terotorisasi, menentukan apakah kinerja sistem dalam kapasitas yang masih dapat diterima oleh pengguna, menentukan adanya kebutuhan baru atas perangkat keras dan lunak.

Nama : Putri Armilia Prayesy

Nim : 182420125

Mata Kuliah : IT Audit

MTI 20A

Untuk proses control (pengendalian) ada tindakan yang perlu dilaksanakan, gunaka referensi yang ada untuk menjawab pertanyaan saya tertutama dalam hal pengembangan sistem, pemrogramaan dan operasional

Jawab :

Tindakn yang perlu dilaksanakan dalam hal pengembangan sistem, pemrograman dan operasional

1. **Pengembangan sistem** bertanggung jawab atas desain, implementasi dan pemeliharaan sistem aplikasi
   a. Mengembangkan prosedur pengendalian yang dapat berfungsi dengan baik.
   b. Penciptaan sistem pengolahan data berbasis komputer secara internal dan eksternal untuk memberikan peluang bagi akses informasi yang menguntungkan manajer sebagai penentu kebijakan
   c. Orientasi strategi yang mengarahkan pada penciptaan terobosan baru dalam kebijkan manajemen dengan memperkecil tingkat hambatan.
   d. Membudayakan pengendalian sebagai suatu program kerja manajemen dan pengembangan sistem terhadap hasil informasi yang disajikan.

2. **Pemrograman** bertanggung jawab atas pemrograman sistem yang baru, memelihara sistem yang lama dan menyediakan perangkat lunak dukungan sistem seperti :
   a. Mendeteksi apakah komputer dikelola secara kurang terarah
   b. Mendeteksi resiko kehilangan data
   c. Mendeteksi resiko informasi yang tidak akurat, berdasarkan data yang salah.
   d. Menjaga aset
   e. Mendeteksi error komputer

3. **Operasional** bertanggung jawab atas perencanaan dan pengendalian operasional harian teknologi informasi melalui:
   a. Identikasi proses-proses
   b. Identifikasi jenis risiko untuk setiap proses
   c. Identifikasi kontrol untuk setiap proses
   d. Evaluasi kecukupan sistem kontrol dalam mitigasi risiko
   e. Menentukan kontrol utama terkait setiap proses
   f. Menentukan efektifitas kontrol utama

Nama : **Putri Eleina Nurrahma**
Nim : **182420138**
Kelas : **MTI. 20A**
DosenPengasuh : **Dr Widya Cholil , S.Kom., M.I.T.**
Mata Kuliah : **IT Audit**

Soal

untuk proses control (pengendalian) ada tindakan yang perlu dilaksanakan, gunaka referensi yang ada untuk menjawap pertanyaan saya tertutama dalam hal pengembangan sistem, pemrogramaan dan operasional.

Jawaban :

Pengendalian umum atau pengendalian manajemen adalah mengevaluasi aspek-aspek pengendalian umum pada TI apakah sudah dilakukan dengan baik oleh manajemen atau belum.

1. Pengembangan Sistem

Suatu hal yang menjadi perdebatan sejak dahulu ialah mengenai hal yang berfokus pada apakah seorang auditor sebaiknya terlibat dalam tim pengembangan selama proses pengembangan sistem.

a. Pendekatan audit pengembangan sistem

Auditor dapat memilih salah satu atau kombinasi dari tiga pendekatan berikut ini:

1. Concurrent Audit , Auditor merupakan bagian dari tim pengembangan sistem. Tugas mereka ialah membantu tim pengembangan meningkatkan kualitas sistem pengembanganny.
2. Post implementation Audit, auditor melakukan audit setelah tahap pengembangan sistem selesai dilakukan. Tujuannya ialah guna mengevaluasi sistem yang nantinya akan dihentikan, dilanjutkan ataupun dimodifikasi,
3. General Audit, Auditor menilai pengendalian atas pengembangan sistem secara keseluruhan. Auditor melakukan pendekatanini dengan tujuan untuk dapat mengurangi banyaknya substantive test yang dilakukan untuk menyatakan pendapat.

b. Evaluasi atas pengembangan sistem

- Defenisi permasalahan

  untuk memastikan apakah perusahaan *(stakeholders)* mengetahui apa resiko dan peluang yang mungkin terjadi terkait dengan penambahan suatu sistem informasi tersebut.

- Manajemen perubahan

  Dengan menitikberatkan pada mempersiapkan perubahan dalam perusahaan dengan pendekatan mendidik *unfreezing the organization)*; berubah ke sistem yang baru *(moving the organization)*; menolong siapa saja yang berkaiatan dengan sistem utnutk beradaptasi dan merasa nyaman dengan sistem yang baru ini *(refreezing the organization)*

- Studi kelayakan

  Perlu dilakukan untuk memperoleh komitmen perubahan dari seluruh bagian yang bakal berubah dan mempelajarai secara *cost-effective* apakah perubahan ini bisa dilakukan atau tidak, dan memastkan tidak akan menimbulkan permasalahan dikemudian hari. Ada 4 studi kelayakan yang erlu dilakukan perusahaan yaitu : technical feasibiity, operational feasibility, economic feasibilty, behavioral feasibility.

- Analisa sistem yang ada

  Jika sistem yang baru akan direkomendasikan untuk menggantikan sistem yang ada maka ada bebeapa hal yang perlu dilakukan perusahaan yaitu : mempelajari latar belakang, struktur dan budaya organisasi yang ada sekarang untuk mendapatkan pemahaman yang matang; mempelajari arus produk dan informasi yang akan diusulkan sis sietem yang baru.

- Menyusun kebutuhan strategis
- Mendesain organisasi dan pekerjaan
- Mendesain sistem pemrosesan informasi, dengan memeriksa enam aktifitas utama, yaitu :
  1. Pendeskripsian kebutuhan strategis untuk meminimalisir ketidakpastian di sekeliling sistem
  2. Memastikan bahwa hasil sistem ini memang benar-benar seperti yang diharapkan dan sesuai rencana

3. Mengevaluasi keputusan dalam ruang lingkup database untuk mendefenisikan hal tersebut akan dilaksanakan atau tidak
4. Memastikan pakah desainer sudah mengikuti suatu standar yang berhubungan dengan bagaimana membuat suatu desain yang baik
5. Menitikberatkan perhatian apakah gambaran fisik desain sudah cukup baik atau tidak
6. Memastikan agar desain yang dibuat bisa terintegrasi dengan baik dengan *hardware* atau *software* yang sudah ada.

- Akuisisi/Pengembangan aplikasi
- Akuisisi perangkat lunak
- Pengembangan prosedur
- Uji penerimaan
- Konversi dan implementasi
- Operasi dan pemeliharaan

2. Pemrograman

1. Karakteristik Pemrograman

Dalam melaksanakan evaluasi atas manajemen pemrograman auditor harus memahami dan memfokuskan perhatiannya pada beberapa karakteristik program yang berkualitas tinggi, yaitu :

- Berfungsi secara benar dan lengkap
- Mempunyai interface pengguna yang berkualitas tinggi
- Bekerja secara efektif
- Didesain dan didokumentasikan dengan baik
- Mudah dipelihara
- Tahan terhadap kondisi yang abnormal

Beberapa hal penting dalam pengendalian manajemen pemrograman adalah:

- Gunakan staf pemrograman yang berkualitas tinggi
- Sedapat mungkin lakukan pemisahan fungsi
- Kembangkan dan dokumentasikan metodologi dan standar kinerja
- Batasi kewenangan programer
- Pelihara log manual dan log komputer atas aktivitas program

- Gunakan konsultan luar untuk mengevaluasi pekerjaan pemrograman
- Lakukan penilaian silang atas kinerja programer secara periodik

2. Evaluasi atas manajemen pemrograman
   a. Tahap perencanaan, Dalam tahap perencanaan yang paling sulit dilakukan adalah perkiraan biaya pemrograman. Audit sebaiknya mengetahui beberapa teknik perkiraan biaya pemrograman.
   b. Tahap Desain, Jika suatu program akan dikembangkan atau dimodifikasi maka pasti akan ada fase desain. Dalam hal ini akan sangat banyak jenis pendekatan desain model, maka diharapkan seorang auditor mengetahui secara umum dan mengapa programmer umumnya menggunakan pendekatan itu.
   c. Tahap Coding, Selama tahap coding ini programmer melakukan penulisan progam yang pada akhirnya akan membuat program itu menjalankan perintah yang kita inginkan. Sejalan dengan semakin besarnya modul yang akan dibuat maka semakin banyak pula modul-modul di dalamnya.
   d. Tahap Testing, Tahap ini di tunjukkan untuk mengidentifikasikan adanya kesalahan, bukan ketidakberadaan kesalahan. Tahap-tahap umum yaitu : memilih batasan pengujian, menentukan sasaran pengujian, memilih pendekatan pengujian, mengembangkan pengujian, melakukan pengujian, mengevaluasi pengujian dan mendokumentasikan pengujian.
   e. Tahap operasi dan pemeliharaan, Beberapa aktifitas utama pada tahap ini yang perlu dievaluasi oleh auditor adalah monitoring kinerja dan jeni-jenis pemeliharaan dan perbaikan yang dilakukan serta pengendalian perangkat lunak manajemen konfigurasi yang digunakan.

3. Operasional

a. Computer Operational Control

   Terdiri dari : **operation control** (untuk menentukan apakah fungsi manusia atau operasi otomasi yang harus dilakukan); **schedulling control** (untuk memastikan ahwa sumber daya hardware yang dimiliki oleh perusahaan digunakan hanya oleh personil yang berhak dan hanya digunakan untuk kepentingan perusahaan saja; **maintenance control** (menentukan bagaimana perangkat keras harus dipelihara untuk mencegah kerusakan dan memfungsikan kembali hardware yang rusak.

b. Network Operation Control

Terdiri dari LAN controls dan WAN Controls. LAN controls berhubungan dengan kegiatan di Local Area Network, dimana manajemen operasi dalam LAN terjadi melalui fasilitas-fasilitas yang diberikan oleh file server. Wan controls merupakan pengendalian jaringan dalam lingkungan yang lebih luas. Ada suatu keadaan dimana operator harus mengidentifkasi kejadian tertentu dan mengkonfigurasi ulang jaringan untuk mengatasi masalah. Alat yang biasanya berguna untuk jaringan bersar ini disebut Network Control Terminal (NCT) dimana hanya hanya operator senior yang terlatih baik yang akan melaksanakan pengendalian guna menjaga keamanan aset dan integritas data dalam NCT.

c. Data Preparation dan Entry

Meliputi :

1. Source document design, dimana sebuah sumber dokumen terstruktur dengan baik, data apa saja yang dicatat, siapa yang mencatat, atau bagaimana dokumen tersebut disimpan ke dalam sistem.
2. Source document storage, dimana sumber yang telah dientry diberi tanda dan tidak boleh dientry kembali dan dikendalikan dengan baik penyimpananya
3. Input screen design, dimana perancangan tampilan layr input disesuaikan dengan dokumen sumber dan meperhatikan kemudahan pengguna dan kecepatan entry data.
4. Data entry area design, dimana desain area pemsukan data harus membuat nyaman operator.

d. Production control

Meliputi receipt & dispatch of input &output, job schedulling, user service level agreement, transfer pricing or charge out control dan computer consumables.

e. File library control

Bertanggung jawab terhadap pengorganisasian penggunaan media penyimpanan, seperti storage of storage media, use of storage media, maintenance and disposal of storage media, location of storage media.

f. Documentation and program library control.

Auditor dapat mengevalusi dengan menanyakan pada *documentation librarians* tetang tugas mereka, bagaiaman mereka mengorganisir penyimpanan dokumentasi danmemeriksa serta memastikan pencatatan dokumentasi berada dalam tempat yang

aman sehingga orang yang tidak bertanggung jawab tidak bisa merubah dan memanfaatkan dokumentasi tersebut.

g. Helpdesk/technical support control.

   Yang berfungsi : membantu end-user menggunakan hardware dan software, menyediakan dukungan teknis bagi sistem produksi dengan membantu memecahkan permasalahan.

h. Mengevaluasi profil kinerja akan adanya aktifitas yang tidak terotorisasi. Auditor mengevaluasi bagaimana manajemen operasi menorganisir perencanaan kapasitas dan fungsi monitor performance. Akan lebih baik jika tersedia catatan statistik mengenai monitor pekerjaan mereka.

i. Management of outsourced operations controls.

   Ada 4 pengendalian jika suatu perusahaan akan melakukan outsourcing, yaitu :

   1. Evaluasi atas kemampuan finansial vendor
   2. Memastikan ketaatan terhadap termin dan kondisi kontrak
   3. Memastikan kemampuan untuk mengendalikan operasi vendor
   4. Menjaga disaster recovery planning

Nama : Rahmad Kartolo
NIM : 182420119
Kelas : MTI Reguler B
Mata Kuliah : IT AUDIT

Untuk proses control (pengendalian) ada tindakan yang perlu dilaksanakan, gunaka referensi yang ada untuk menjawap pertanyaan saya tertutama dalam hal pengembangan sistem, pemrogramaan dan operasional

Penyelesaian:

A. Kontrol Administratif

Kontrol administratif dimaksudkan untuk menjamin bahwa seluruh kerangka control dilaksanakan sepenuhnya dalam organisasi berdasarkan prosedur-prosedur yang jelas. Kontrol ini mencakup hal-hal berikut:

- ✓ Mempublikasikan kebijakan control yang membuat semua pengendalian sistem informasi dapat dilaksanakan dengan jelas dan serius oleh semua pihak dalam organisasi.
- ✓ Prosedur yang bersifat formal dan standar pengoperasian disosialisasikan dan dilaksanakan dengan tegas. Termasuk hal ini adalah proses pengembangan sistem, prosedur untuk backup, pemulihan data, dan manajemen pengarsipan data.
- ✓ Perekrutan pegawai secara berhati-hati yang diikuti dengan orientasi pembinaan, dan pelatihan yang diperlukan.
- ✓ Supervisi terhadap para pegawai. Termasuk pula cara melakukan control kalau pegawai melakukan penyimpangan terhadap yang diharapkan.
- ✓ Pemisahan tugas-tugas dalam pekerjaan dengan tujuan agar tak seorangpun yang dapat menguasai suatu proses yang lengkap. Sebagai contoh, seorang pemrogram harus diusahakan tidak mempunyai akses terhadap data produksi (operasional) agar tidak memberikan kesempatan untuk melakukan kecurangan.

B. Kontrol Pengembangan dan Pemeliharaan Sistem

Untuk melindungi kontrol ini, peran auditor sangat sistem informasi sangatlah penting. Auditor system informasi harus dilibatkan dari masa pengembangan hingga pemeliharaan system, untuk memastikan bahwa system benar-benar terkendali, termasuk dalam hal otorisasi pemakai system. Aplikasi dilengkapi dengan audit trail sehingga kronologi transaksi mudah untuk ditelusuri.

C. Kontrol Operasi

Kontrol operasi dimaksudkan agar system beroperasi sesuai dengan yang diharapkan. Termasuk dalam kontrol ini:

- ✓ **Pembatasan akan akses terhadap data**

  Akses terhadap ruangan yang menjadi pusat data dibatasi sesuai dengan wewenang yang telah ditentukan. Setiap orang yang memasuki ruangan ini harus diidentifikasi dengan benar. Terkadang ruangan ini dipasangi dengan CTV untuk merekam siapa saja yang pernah memilikinya.

- ✓ **Kontrol terhadap personel pengoperasi**

  Dokumen yang berisi prosedur-prosedur harus disediakan dan berisi pesoman-pedoman untuk melakukan suatu pekerjaan. Pedoman-pedoman ini arus dijalankan dengan tegas. Selain itu, [ara [ersonel yang bertugas dalam pengawasan operasi sistem perlu memastikan bahwa catatan-catatan dalam sistem komputer (system log) benar-benar terpelihara.

- ✓ **Kontrol terhadap peralatan**

  Kontrol terhadap peralatan-peralatan perlu dilakukan secara berkala dengan tujuan agar kegagalan peralatan dapat diminimumkan.

- ✓ **Kontrol terhadap penyimpanan arsip**

  Kontrol ini untuk memastikan bahwa setiap pita magnetic yang digunakan untuk pengarsipan telah diberi label dengan benar dan disimpan dengan tata cara yang sesuai.

- ✓ **Pengendalian terhadap virus**

  Untuk mengurangi terjangkitnya virus, administrator sistem harus melakukan tiga kontrol berupa preventif, detektif, dan korektif.

E. Kontrol Perangkat Keras

Untuk mengatisipasi kegagalan sistem komputer, terkadang organisasi menerapkan sistem komputer yang berbasis fault-tolerant (toleran terhadap kegagalan). Sistem ini dapat berjalan sekalipun terdapat gangguan pada komponen-komponennya. Pada sistem ini, jika komponen dalam sistem mengalami kegagalan maka komponen cadangan atau kembarannya segera mengambil alih peran komponen yang rusak dan sistem dapat melanjutkan operasinya tanpa atau dengan sedikit interupsi.

Sistem fault-tolerant dapat diterapkan pada lima level, yaitu pada komunikasi jaringan, prosesor, penyimpan eksternal, catu daya, dan transaksi. Toleransi kegagalan terhadap jaringan dilakukan dengan menduplikasi jalur komunikasi dan prosesor komunikasi. Redundasi prosesor dilakukan antaralain dengan teknik watchdog processor, yang akan mengambil alih prosesor yang bermasalah.

Toleransi terhadap kegagalan pada penyimpan eksternal antara lain dilakukan melalui disk memoring ataudisk shadowing, yang menggunakan teknik dengan menulis seluruh data ke dua disk secara pararel. Jika salah satu disk mengalami kegagalan, program aplikasi tetap bisa berjalan dengan menggunakan disk yang masih bai. Toleransi kegagalan pada catu daya diatasi melalui UPS. Toleransi kegagalan pada level transaksi ditanganimelalui mekanisme basis data yang disebut rollback, yang akan mengembalikan ke keadaan semula yaitu keadaan seperti sebelum transaksi dimulai sekiranya di pertengahan pemrosesan transaksi terjadi kegagalan.

F. Kontrol Akses terhadap Sistem computer

untuk melakukan pembatasan akses terhadap sistem, setiap pemakai sistem diberi otorisasi yang berbeda-beda. Setiap pemakai dilengkapi dengan nama pemakai dan password. Password bersifat rahasia sehingga diharapkan hanya pemiliknyalah yang tahu password-nya. Setelah pemakai berhasil masuk ke dalam sistem (login), pemakai akan mendapatkan hak akses sesuai dengan otoritas yang telah ditentukan. Terkadang, pemakai juga dibatasi oleh waktu. Kontrol akses juga bisa berbentuk kontrol akses berkas. Sebagai contoh, administrator basis data mengatur agar pemakai X bisa mengubah data A, tetapi pemakai Y hanya bisa membaca isi berkas tersebut.

Jika pendekatan tradisional hanya mengandalkan pada password, sistem-sistem yang lebih maju mengombinasikan dengan teknologi lain. Misalnya, mesin ATM (anjungan tunai mandiri) menggunakan kartu magnetic atau bahkan kartu cerdas sebagai langkah awal untuk mengakses sistem dan kemudian baru diikuti dengan pemasukan PIN (personal identification number). Teknologi yang lebih canggih menggunakan sifat-sifat biologis manusia yang bersifat unik, seperti sidik jari dan retina mata, sebagai kunci untuk mengakses sistem.

Pada sistem yang terhubung ke Internet, akses Intranet dari pemakai luar (via Internet) dapat dicegar dengan menggunakan firewall. Firewall dapat berupa program ataupun perangkat keras yang memblokir akses dari luar intranet.

G. Kontrol terhadap Akses Informasi

Ada kemungkinan bahwa seseorang yang tak berhak terhadap suatu informasi berhasil membaca informasi tersebut melalui jaringan (dengan menggunakan teknik sniffer). Untuk mengantisipasi keadaan seperti ini, alangkah lebih baik sekiranya informasi tersebut dikodekan dalam bentuk yang hanya bisa dibaca oleh yang berhak. Studi tentang cara mengubah suatu informasi ke dalam bentuk yang tak dapat dibaca oleh orang lain dikenal dengan istilah kriptografi. Adapun sistemnya disebut sistem kripto. Secara lebih khusus, proses untuk mengubah teks asli (cleartext atau plaintext) menjadi teks yang telah dilacak (cliphertext) dinamakan enskripsi, sedangkan proses kebalikannya, dari chiphertext menjadi cleratext,disebut dekrpisi.

Nama :Reynaldi Tugas : IT Audit

NIM : 182420111 (MTI REG B 2019) Tanggal : 2 April 2020

SOAL

untuk proses control (pengendalian) ada tindakan yang perlu dilaksanakan, gunakan referensi yang ada untuk menjawap pertanyaan saya tertutama dalam hal pengembangan sistem, pemrogramaan dan operasional

JAWAB

Dalam proses pengendalian dalam hal pengembangan sistem, pemrograman dan operasional memiliki manajemen nya tersendiri, dak berikut adalah manajemen dalam pengendalian pengembangan sistem, pemrograman dan operasional :

1. **Manajemen Pengembangan Sistem**
   Suatu hal yang menjadi perdebatan sejak dahulu ialah mengenai hal yang berfokus pada selama proses pengembangan sistem. Bagi yang mendukung hal ini memerikan argumen karena di tahap inilah kesalahan-kesalahan sebaiknya diperbaiki. Sebaliknya beagi yang menolak berargumen tidak sepasntasnya siapa yang bakao meng-audit sistem ini nantinya turut serta ula membangun sistem ini karen menimbulkna *conflict of interest* pada saat audit.

   1.1. Pendekatan Audit atas pengembangan Sistem

   Auditor adapat memlih salah satu atau kombinasi dati tiga pendekatan berikut ini dalam melakukan audit atas pengembangan sistem :

   - **Conurrent Audit -** Auditor merupakan bagian dari tim pengembangan sistem. Tugas mereka ialah membantu tim pengembangan meningkatkan kualitas sistem pengembangannya.
   - **Post Implementation Audit** - Auditor melakukan audit setelah tahap pengembangan sistem selesai dilakukan. Tujuannya ialah guna mengevluasi sistem yang nantinya akan dihentikan, dilanjutkan ataupun dimodifikasi.
   - **General Audit** – Auditor menilai pengendalian atas pengembanga sistem secara kesuluruhan untuk dapat mengurangi banyaknya *substantive test* yang dilakukan untuk menyatakan.

1.2 Evaluasi atas pengembangan Sistem

Definisi Permasalahan – Sistem informasi dibuat untuk mengatasi permasalahan ataupun mengambil keuntungan dari peluang yang ada.

Auditor musti mempunyai empat (4) keingintahuan dibenaknya dalam menyikpi hal ini, yaitu:

- Apakah kemungkinan penyelesaian sistem informasi akan berdampak material dalam hal besar dan pengaruh terhadap perushaan? Kalau ya apakah sudah diberitahukan pada seluruh jajaran perusahaan (stakeholder).
- Jika nantiya sistem informasi akan merubah jalannya perusahaan pada tingkat nama sajakah yang akan berubah?
- Jika nantinya sistem informasi memiliki ketidakpastioan mengenai teknologi yang digunakan, apakah sudah diambil tindakan untuk mengurangi ketidakpastian itu?
- Apkah seluruh jajaran perusahaan (stakeholder) setuju pada pendefinisian masalah dan peluang yang ada? Jika tidak tindakan apa yang diambil oleh manajemen untuk mengambil jalan tengahnya?

Tujuan keingintahuan ini ialah untuk memastikan apkah perusahaan (stakeholder) mengetahui apa resiko dan peluang yang mungkin terjadi terkait dengan penambahan suatu sistem informasi tersebut.

Manajemen Perubahan - Manajemen perubahan berjlan bersamaan dengan semua proses dalam pengembangan sistem. Ada tiga (3) aktivitas yang perlu dilakukan perusahaan selama perubahan ini yaitu:

- **Unfreezing the organization** – yaitu memperisapkan perubaan dalam perushaan dengan pendektan mendidik.
- **Moving the organization** – yaitu berubah ke sistem yang baru dibuat.
- **Refreezing the organization** – yaitu menolon siapa saja yang berkaitan dengan sistem ini untuk pegamatan dan meras nyaman dengan sistem yang baru.

Selama proses ini auditor mentikeratkan pengamatan pada proses tansdormasi ini.

Studi kelayakan – Tujuan dari bagian ini ialah untuk memperoleh komitmen perubahan dari seluruh bagian yang bakal berubah dan mempelajari secara cost-effective apakah perubahan ini masih bisa dilakukan atau tidak. Ada empat (4) studi kelaykan yang perlu dilakukan oleh perusahaan yaitu:

- **Technical Feasibility –** Apakah teknologi yang ada saat ini sanggup menajalankan sistem yang akan dibuat? Dapatkah tehnologi tersebut dibuat dan dilaksanakan?
- **Operasioal Feasibility –** Apakah data yang dimasukkan ke sistem dapat dikumpulkan oleh sitstem? Apakah hasilnya dapat berguna?
- **Economic Feasibility –** Apakah biaya pembuatan sistem ini nantinya akan leih kecil dari manfaat yang akan didapatkan dari sistem ini nantinya?
- **Behavioral Feasibility –** Dampak apa seajakah yang akan terjadi pada pengguna?

Auditor dala hal ini untuk memastikan apakah semua studi kelayakan ini mempunyai hasil yang baik kaena kalau tidak akan menimbulkan permasalaan di kemudian hari.

Nama :Reynaldi
NIM : 182420111 (MTI REG B 2019)
Tugas : IT Audit
Tanggal : 2 April 2020

2. Manajemen Pemrograman

2.1. Karakteristik Pemrograman

Dalam melaksanakan evaluasi atas manajemen pemrograman auditor harus memahamo dan memfokuskan perhatiannya pada beberpa karakteristik program yang berkualitas tinggi, yaitu :

- Berfungsi secara benar dan lengkap
- Mempunyai interfae pengguna yang berkualitas tinggi
- Bekerja scara efektif
- Didesain dan di dokumentasikan dengan baik
- Mudah dipelihara
- Tahan terhadap kondisi yang abnormal

Pengendalian atas manajemen perograman dapat dilakuka dengan memonitoring tahapan-tahapan yang ditempuh dibandingkan dengan rencana untuk memastikan efisiensi dan ketepatan waktu serta menilai pengendalian yang ada untuk memastikan autentikasi, akurasi dan kelengkapan. Monitoring dapat dilakukan menggunakan *work breakdown structure, gantt charts* dan *Evaluation & Review technique* (PERT).

Beberapa hal penting dalam pengendalian manajemen pemrograman antara lain adalah :

- Gunakan staf pemrograman yang berkualitas tinggi
- Sedang mungkin lakukan pemisahan fungsi
- Kembangkan dan dokumentasikan metodologi dan standar kinerja
- Batasi kewenagan programer
- Pelihara log manual komputer atas aktivitas programer
- Gunakan konsultan luar untuk mengevaluasi pekerjaan pemrograman
- Lakukan penilaian silang atas kinerja programer secara periodik

2.2. Evaluasi atas Manajemen Pemrograman

Tahap perencanaan – Dalam tahap perencanaan yang paling sulit dilakuakn adalah perkiraan biaya pemrograman. Auditor sebaiknya mengetahui beberapa teknik biaya pemrograman, antara lain :

- **Algorithmic Models –** Model ini mengestimasikan sumber data yang diperlukan berdasarkan "cost drivers" nya contohnya estimasi jumlah sumber instruksi yang akan ditulis, bahasa pmerograman apa yang digunakan, dll. Contoh model ini ialah Boehm's COCOMO model..
- **Expert Judgement –** seorang yang ahli dalam hal ini mengestimasi sumber-sumber daya yang diperlukan dalam proyek programming.
- **Analogy –** Jika proyek yang sama telah pernah dibuat maka sumber daya yang akan diperlukan di estimasikan berdasarkan proyek-proyek kecil tersebut.
- **Top-down Estimation** – Pertama proyek dibagi atas tugas-tuhas dan sumer daya yang diperlukan di estimasikan berdasarka proyek-proyek.
- **Bottom-up Estimation –** Apabila dari awah sudah dijelaskan dangan sangat detail apa-apa saja uang haru dikerjakan, maka dari sana isa dibuat esrimasi kebutuhab sumber dayanya dan dengan menyatukan seua itu akan didapakan estimasi sumber daya keseluruhan pembuatan sistem.

Disamping mengestimasikan sumber daya yang akan digunakan, manajemen juga harus mendiskusikan beberapa pendekatan dibawah ini :

- **Pendekatan Desain –** Jika pemrograman akan duat in-house maka manajemen harus menetukan pendeketan apa yang akan dipakai top-down, atau bottom-up, atau yang lain.
- **Pendekaran Implementasi –** Software daoar dibuat in-house dikontrakan atau dibeli. Bahasa pemrograman apa yang harus dipilih.
- **Pendekatan Integrasi & Testing –** Test memerlukan semcam alat pencatat kinerja, dan tanggung jawab integrasi juga perlu dirumuskan atau memutuskan pengadaan software, maka keanggotaan dan struktur timnya harus dijelaskan.

Sebagai auditor dalam dase ini mempunyai dua perhatian yaitu mengevaluasi apakah tingkay dari perencanaan sudah cukup dalam setiap usulan aplikasi yang direncarankan. Hal yang kedua ialah auditor harus memastikan seberapa baikah perencanaan kerja tersebut dilaksanakan.

3. Manajemen Operasi

3.1. Computer Operation Control

Operation Control – Pengendalian ini menentukan apakah fungsi manusa atau operasi otomasi yang harus dilakukan banyak jenis aktivitas yang harus dilakukan untuk mendukung jalannya program dikomputer, contohnya : program-program harus dijalankan ataupun dihentikan, media penyimpanan harus di isi dengan data yang *up-to-date*, berbagai formulis dan dokumen herus di cetak *printer* dan lain sebagainya.

Dijaman yang modern ini ada juga kemungkinan penggunaan *automated operations facilities* (AOFs) yang melakukan semua pekerjaan manual diatas secara otomatis. Campur tangan manusia yang akan menjadi semakin kecil jika sudah menggunakan AOFs ini.

Jenis-jenis operasi diatas tersebut adalah oprasi normal kompute. Ketika semakin banyak operasi komputer dilakukan secara terotomatis, auditor harus menitikeratkan pemeriksaan pada masalah-masalah authetifikasi, akurasi, dan kelengkapan dari progam yang erjalan terotomatis tersebut. Pertanyaan yang harus diyakinkan terjawa oleh auditor ialah:

- Siapa yang bertanggung jawab atas desai, implementasi, dan pemeliharaan dari AOFs ini?
- Apakah sewaktu mendesain, mengimplementasi, dan memlihara terdapar standar standat tertentu yang dipatuhi?

Nama :Reynaldi
NIM : 182420111 (MTI REG B 2019)
Tugas : IT Audit
Tanggal : 2 April 2020

- Apakah AOFs dipelihara dalam lingkungan yang aman?
- Seberapa baikkah lingkungan AOFs di dokumentasikan?
- Apakah ada salinan dari dokumen lingkungan AOFs yang dibuat sebagai *back-up* dan dipisahkan di tempat yang lain?

Nama : Rio Permata
NIM : 182420108
Kelas : MTI Reguler B
Mata Kuliah : IT Audit

PROSES PENGENDALIAN PADA PENGEMBANGAN SISTEM, PEMROGRAMAN DAN OPERASIONAL

Pengendalian umum dalam IT Audit adalah proses untuk mengevaluasi aspek-aspek pada IT dalam perusahaan apakah sudah dilakukan dengan baik atau belum. Dalam sebuah perusahaan ada banyak bagian yang perlu dilakukan pengendalian umum IT audit, pada tugas kali ini akan dibahas pengendalian umum pada bagian Pengembangan Sistem, Pemrograman dan Operasional pada Aplikasi GOJEK. GOJEK sebagai salah satu Unicorn di Indonesia berencana untuk melakukan ekspansi terhadap bisnis nya. Dengan cara mengembangkan dan menambah fitur-fitur dalam aplikasi GOJEK yang pada awalnya hanya memiliki fitur GoRide, dan GoCar saja sekarang berencana menambah fitur GoFood, GoSend, dan GoShop.

1. Pengembangan Sistem

1.) Pendekatan audit atas pengembangan sistem

- Concurrent Audit : Auditor menjadi bagian dari tim pengembangan system aplikasi GOJEKk dan bertugas untuk membantu meningkatkan kualitas system aplikasi GOJEK yang dikembangkan.
- Post Implementation Audit : Setelah tahap pengembangan sistem selesai maka auditor melakukan audit yang bertujuan mengevaluasi system aplikasi GOJEK yang telah dibuat, apakah dihentikan, dilanjutkan atau diperbaiki.
- General Audit : Auditor melakukan penilaian pada system aplikasi GOJEK secara keseluruhan.

2.) Evaluasi pengembangan system

- **Mendefinisikan Permasalahan :** Pada tahap ini auditor akan di definisikan system aplikasi GOJEK yang telah dibuat apakah telah berdampak material yang besar bagi perusahaan. Serta peluang dan resiko apa saja yang akan dihadapi terkait perubahan dan penambahan fitur dari aplikasi GOJEK tersebut.
- **Managemen Perubahan :** Pada tahap ini auditor minitikberatkan pengamatan pada masa transisi penambahan fitur GoFood, GoSend, dan GoShop. Seperti

persiapan transisi ke fitur baru serta seberapa paham karyawan akan fitur baru yang akan diterapkan.

- **Studi Kelayakan :** Pada tahap ini auditor memastikan apakah fitur baru yang dibuat dapat sejalan dengan teknologi yang ada pada perusahaan, apakah biaya yang dikeluarkan lebih kecil dari manfaat yang didapat, dan dampak apa saja yang terjadi pada pengguna.
- **Analisa Sistem Yang Ada :** Dalam hal ini auditor akan menitik beratkan perhatian pada tiga hal yaitu : (1) Mengevaluasi tanggapan dari Stakeholders terhadap usulan fitur baru dari Aplikasi Gojek. (2) Auditor memerriksa apakah stakeholders menggunakan metode yang baik dalam menanggapi usulan yang diajukan. (3) Auditor harus memeriksa apakah designer aplikasi menggunakan alat perancangan yang baik dalam membuat desain fitur baru yang diusulkan.
- **Menyusun Kebutuhan Strategis :** Auditor dalam hal ini harus memusatkan perhatiannya pada apakah desainer aplikasi menyadari pentingnya kebutuhan strategis perusahaan
- **Mendesain Organisasi dan Pekerjaan :** Terkadang, untuk mencapai kebutuhan strategis desain atau desain ulang dari struktur organisasi dan pekerjaan. Oleh karena itu auditor harus memastikan kembali hal tersebut
- **Mendesain Sistem Pemrosesan Informasi :** Pada tahap ini dilakukan evaluasi fase desain fitur baru GOJEK, seperti dalam hal Design Interface, Design Database dan lain-lain agar berjalan sesuai dengan yang telah direncanakan dan disepakati.
- **Pengembangan Aplikasi :** Fitur baru GOJEK yang didesain harus di evaluasi dengan seksama oleh auditor secara prosedur dalam desain, koding, testing, dokementasi dan lain-lain
- **Akuisisi Perangkat Keras dan Lunak :** Dalam pengembangan fitur baru dari aplikasi GOJEK diperlukan hardware dan software yang pengadaanya dilakukan melalui proposal. Tugas auditor untuk memastikan bahwa proposal itu telah dibuat dan dipersiapkan dengan baik.
- **Pengembangan Prosedur :** Jika fitur baru dari aplikasi GOJEK memiliki dampak yang besar terhadap perusahaan maka tugas auditor adalah memastikan prosedur dari fitur baru itu tersedia untuk berbagai tingkatan level.

- **Uji Penerimaan :** Untuk mengidentifikasi apakah ada masalah dan penyimpangan yang terjadi dalam proses menuju versi final dari fitur baru aplikasi GOJEK.
- **Konversi dan Implementasi :** Auditor harus memastikan implementasi fitur baru ke aplikasi GOJEK harus berjalan dengan baik sesuai dengan rencana yang telah ditetapkan
- **Operasi dan Pemeliharaan :** Perhatian utama auditor dalam hal ini adalah proses perbaikan dan pemeliharaan aplikasi dapat tercatat dengan baik demikian juga pengendalian atas perbaikan dan pemeliharan tersebut harus tercatat juga.

2. Managemen Pemrograman

1.) Evaluasi managemen pemrograman

- Algorithmic Models : auditor melakukan estimasi jumlah serta Bahasa pemrograman yang akan digunakan pada system aplikasi GOJEK yang sedang dikembangkan.
- Expert Judgement : melakukan estimasi terhadap sumberdaya yang diperlukan dalam proses pengembangan aplikasi GOJEK
- Analogy : Jika sebelumnya proyek pengembangan yang sama pernah dibuat maka dapat estimasi dapat merujuk kesana
- Top – Down Estimation : proyek dibagi atas tugas – tugas kecil, dan sumber daya diestimasikan berdasarkan proyek kecil tersebut
- Bottom – Up Estimation : mendefinisikan dengan sangat detil hal apa yang harus dikerjakan sehingga dapat diestimasikan sumber daya nya.

2.) Tahap Testing / Pengujian

- Unit Testing : memfokuskan evaluasi pada individual modul dalam program
- Integration Testing : Test yang memfokuskan pengujian pada evaluasi sejumlah modul program secara bersama-sama

- Whole of Program Testing : Test yang memfokuskan pada seluruh program secara total

3. Managemen Operasional

- Operation Control : pengendalian ini menentukan apakah fungsi manusia atau operasi otomasi yang harus dilakukan.
- Scheduling Control : pengendalian ini yang menentukan bagaimana sebuah pekerjaan harus dijadwalkan dalam lingkungan platform perangkat keras dan lunak.
- Maintenance Control : pengendalian terhadap pemeliharaan hardware dari system.
- Network Operation Control : pengendalaian terhadap jaringan system yang telah berjalan.
- Data Preparation & Entry : pengendalian terhadap proses pencatatan data
- File Library Control : pengendalian yang bertanggung jawab terhadap pengorganisasian penggunaan media penyimpanan
- Documentation & Program Library Control : bertanggung jawab terhadap pengorganisasian dokementasi operasional perusahaan

PROSES CONTROL YANG PERLUDILAKUKAN DALAM HAL PENGEMBANGAN SISTEM,PEMROGRAMAN,DAN OPERASIONAL

Proses control dalam pengembangan system

1. Manajemen perubahan-dimana dalam proses ini ada 3 poin yang harus dilakukan perusahaan dalam perubahan yaitu:
   - Unfreezing the organization
   - Moving the organization
   - Refreezing the organization
2. Study kelayakan bisnis: dimana dalam proses ini ada 4 poin yang harus dilakukan oleh perusahaan yaitu:
   - Technical Feasibility
   - Operational Feasibility
   - Economic Feasibility
   - Behavioral Feasibility
3. Analisis system yang ada:dalam menganalisis system ada beberapa hal yang harus dilakukan oleh perusahaan yaitu:
   - Mempelajari latar belakang struktur dan budaya organisasi
   - Mempelajari arus produk dan informasi
   - Menyusun Kebutuhan Strategis
   - Mendesain Organisasi dan Pekerjaan

Proses control dalam manajemen pemrograman

Beberapa hal penting dalam pengendalian manajemen pemrograman antara lain adalah :

- Gunakan staf pemrograman yang berkualitas tinggi
- Sedapat mungkin lakukan pemisahan fungsi
- Kembangkan dan dokumentasikan metodologi dan standar kinerja
- Batasi kewenangan programer
- Pelihara log manual dan log komputer atas aktivitas programer
- Gunakan konsultan luar untuk mengevaluasi pekerjaan pemrograman
- Lakukan penilaian silang atas kinerja programer secara periodik

Proses control manajemen oprasional

Adapun Proses control dalam manajemen operasional adalah sebagai berikut:

1. Scheduling Control
2. Maintenance Control

3. LAN Controls
4. WAN Controls
5. File Library Control
6. Documentation & Program Library Control
7. Help Desk/Technical Support Control
8. Capacity Planning and Performance Monitoring Control

IT AUDIT (MTIK319)

CONTROL DAN AUDIT TI

Nama :

Yudistira Sira Permana 182420104

Dosen :

Dr. Widya Cholil, S.Kom., M.IT

Universitas Binda Darma

MTI 20 Reguler A

DAFTAR ISI

CONTROL DAN AUDIT TI

1. TI Dalam peningkatan Pengendalian Internal

Kebanyakan entitas, termasuk bisnis kecil yng dimiliki keluarga berdasar pada TI untuk mencatat dan memproses transaksi bisnis. Sebagai hasil kemajuan luar biasa dalam di dalam TI, bahkan bisnis yang relatif sederhana menggunakan komputer pribadi dengan perangkat lunak akuntansi yang dibeli untuk proses akuntansi mereka. Penggunaan lingkungan jaringan yang kompleks, internet dn fungsi TI terpusat adalah umum dalam bisnis saat ini. Beberapa perubahan pengendalian internal yang diakibatkan oleh pengintegerasian TI ke dalam sistem akuntansi :

1.1. Kendali komputer menggantikan kendali manual.

Mamfaat yang nyata dari TI, seperti kemampuan untuk menangani volume yang luar biasa dari transaksi bisnis yang rumit secara hemat biaya, menyebabkan organisasi untuk menggunakan TI sepanjang proses pelaporan keuangan mereka. Satu keuntungan TI adalah kemampuan untuk meningkatkan pengendalian internal dengan menggabungkan kendali yang dilakukan komputer dalam aktivitas proses transaksi sehari-hari. Menggantikan prosedur manual dengan pengendalian yang diprogramkan yang menggunakan cek dan saldo bagi masing-masing transaksi yang diproses dapat mengurangi kesalahan manusia yang mungkin terjadi dalam lingkungan manual yang tradisional. Suatu sistem TI yang terkendali menawarkan potensi lebih besar untuk mengurangi salah saji karena komputer memroses informasi secara konsisten. Contoh dari pengendalian internal yang dilakukan oleh komputer yang pernah diproses oleh karyawan sedang membandingkan pelanggan dan nomor produk dengan arsip induk dan membandingkan jumlah transaksi penjualan dengan batas kredit yang telah diprogram. Pengendalian keamanan online dalam aplikasi, data-base, dan sistem operasional juga menyediakan peluang untuk meningkatkan pemisahan dari kewajiban.

1.2. Tersedianya informasi dengan mutu lebih tinggi.

Sekali manajemen yakin tentang keandalan informasi yang dihasilkan oleh TI, penggunaan manajemen atas informasi itu menawarkan potensi lebih lanjut untuk meningkatkan keputusan manajemen. Pertama-tama, lingkungan TI yang kompleks umumnya diatur secara efektif karena kompleksitas memerlukan

organisasi yang efektif, prosedur, dan dokumentasi. Kedua, sistem TI biasanya menyediakan bagi manajemen lebih banyak informasi dengan mutu lebih tinggi dengan lebih cepat dari kebanyakan sistem manual.

2. Resiko yang Muncul dari Penggunaan Sistem Akuntansi Berbasis TI

Meskipun IT meningkatkan pengendalian intern perusahaan, hal ini juga dapat mempengaruhi resiko-resiko pengendalian perusahaan secara keseluruhan. resiko khusus pada sistem TI yaitu:

2.1. Resiko pada perngkat keras

Meskipun IT memberikan manfaat pemrosesan yang signifikan, hal itu juga menciptakan resiko yang unik dalam melindungi perangkat keras dan data, termasuk potensi munculnya jenis kesalahan baru. Resiko khusus ini mencakup hal-hal berikut:

a. Ketergantungan pada kemampuan berfungsinya perangkat keras dan lunak.
b. Kesalahan sistematis versus kesalahan acak
c. Akses yang tidak sah salah
d. Hilangnya data

2.2. Jejak audit yang berkurang

Salah saji mungkin tidak terdeteksi dengan meningkatnya penggunaan IT akibat hilangnya jejak audit secara nyata , termasuk berkurangnya keterlibatan manusia. selain itu, computer juga menggantikan jenis otorisasi tradisional dalam banyak sistem IT.

a. Visibilitas jejak audit. karena sebagian besar informasi dimasukan secara langsung ke dalam computer, penggunaan IT sering kali mengurangi atau bahkan meniadakan dokumen dan catatan sumber yang memungkinkan organisasi menelusuri informasi akuntansi.
b. Keterlibatan Manusia yang berkurang. Dalam banyak sistem IT, karyawan yang terlibat dengan pemrosesan awal transaksi tidak pernah melihat hasil akhirnya. Karena itu, mereka kurang mampu mengidentifikasi salah saji pemrosessan, Walapun mereka melihat outout akhir, sering kali sulit untuk mengenali salah saji karena hasilnya sering sangat ringkas.

c. Tidak adanya otorisasi traditiona. Sistem IT yang sangat canggih biasanya diprakarsai jenis transaksi tertentu secara otomatis, seperti perhitungan bunga atas rekening tabungan bank dan pemesanan persediaan apabila tingkat pesanan yang dtentukan telah dicapai,

2.3. Kebutuhan IT akan pengalaman dan pemisahan tugas

Sistem IT mengurangi sistem pemisahan tugas traditional (otorisasi, pembukuan, penyimpanan) dan menciptakan kebutuhan akan pengalaman IT tambahan.

3. Pengendalian Khusus atas Teknologi Informasi

Untuk menunjuk banyak dari risiko yang berhubungan dengan kepercayaan lebih besar atas TI, organisasi sering mengimplementasikan pengendalian khusus untuk fungsi TI. Standar audit menjelaskan dua pengelompokan pengendalian yang utama untuk sistem TI: pengendalian umum dan pengendalian aplikasi.

3.1. Pengendalian Umum (General Control)

merupakan sistem pengendalian internal komputer yang berlaku umum dimana kegiatannya meliputi seluruh kegiatan komputerisasi sebuah perusahaan secara menyeluruh. Auditor biasanya mengevaluasi pengendalian umum diawal audit oleh karena dampak dari pengendalian umum atas pengendalian aplikasi. Keenam kategori dari pengendalian umum kini diuji secara lebih detail. Keenam kategori tersebut adalah :

a. Administrasi dari Fungsi TI.
b. Pemisahan Tugas-tugas TI.
c. Pengembangan sistem.
d. Kemanan fisik dan online.
e. Backup dan Perencanaan Kontijensi
f. Pengendalian Perangkat Keras.

3.2. Pengendalian Aplikasi (Application Control),

merupakan sistem pengendalian internal (internal Controls) pada sistem informasi berbasis teknologi informasi yang berkaitan dengan pekerjaan / kegiatan /aplikasi tertentu diamana setiap aplikasi mempunyai karakteristik tertentu dan kebutuhan pengendalian yang berbeda.

Pengendalian aplikasi dirancang untuk masing-masing aplikasi perangkat lunak dan dimaksudkan untuk membantu sebuah perusahaan memenuhi enam sasaran hasil audit yang terkait dengan transaksi. Walaupun beberapa pengendalian aplikasi mem- pengaruhi satu atau hanya beberapa sasaran hasil audit yang terkait dengan transaksi, kebanyakan kendali mencegah atau mendeteksi beberapa jenis salah saji.

Pengendalian aplikasi bisa dilakukan oleh komputer atau oleh manusia. Pengen-dalian aplikasi yang dilakukan oleh manusia yang berinteraksi dengan komputer sering dikenal sebagai pengendalian pemakai. Efektivitas dari pengendalian pemakai, seperti tinjauan ulang dari laporan pengecualian yang dihasilkan-komputer, sering tergantung pada akurasi dari informasi yang dihasilkan. Pengendalian aplikasi terdiri dari tiga kategori, yaitu :

1. Pengendalian input
2. Pengendalian Pemrosesan
3. Pengendalian output

Pengendalian umum di-rancang untuk melindungi semua pengendalian aplikasi untuk memastikan bahwa pengendalian itu efektif. Pengendalian umum yang kuat mengurangi jenis risiko yang dikenali di kotak di luar bentuk oval pengendalian umum.

4. Dampak Teknologi Informasi Pada Proses Audit

Auditor harus memiliki banyak pengetahuan tentang pengendalian ini sebab mereka bertanggung jawab atas perolehan suatu pemahaman dari pengendalian internal, termasuk pengendalian umum dan pengendalian aplikasi, dengan mengabaik- an apakah penggunaan TI oleh klien adalah kompleks atau sederhana. Juga, pe- ngetahuan tentang pengendalian umum meningkatkan kemampuan auditor untuk ber- sandar pada pengendalian aplikasi efektif untuk mengurangi risiko pengendalian untuk sasaran hasil audit yang terkait dengan transaksi.

4.1. Pengaruh dari Pengendalian Umum oleh Risiko Pengendalian

Kebanyakan auditor mengevaluasi efektivitas dari pengendalian umum sebelum mengevaluasi pengendalian aplikasi. Jika pengendalian umumnya tidak efektif, ada potensi untuk salah saji material pada setiap aplikasi akuntansi yang berbasis kompu- ter, dengan mengabaikan mutu dari pengendalian aplikasi.

Auditor biasanya memperoleh informasi tentang pengendalian umum dan aplikasi melalui wawancara dengan personil TI dan para pemakai kunci; pengujian dokumentasi sistem seperti bagan alur, manual pemakai, permohonan perubahan program, dan hasil pengujian; dan tinjauan ulang dari daftar pertanyaan terperinci yang diselesaikan oleh staf TI. Dalam banyak kasus, diinginkan untuk menggunakan beberapa pendekatan dalam pemahaman pengendalian internal karena masingmasing menawarkan informasi yang berbeda. Wawancara dengan pejabat kepala informasi dan analis sistem menyediakan informasi yang bermanfaat tentang pengoperasian keseluruhan fungsi TI, tingkat dari pengembangan perangkat lunak dan perangkat keras yang dibuat untuk perangkat lunak aplikasi akuntansi kunci, dan suatu ikhtisar dari perubahan yang direncanakan. Tinjauan ulang dari program mengubah per- mintaan dan hasil percobaan sistem adalah bermanfaat dalam mengidentifikasikan perubahan program dalam perangkat lunak aplikasi. Daftar Pertanyaan berguna untuk mengidentifikasikan pengendalian internal yang spesifik.

4.2. Efek dari Pengendalian TI atas Risiko Pengendalian dan Ujian Substantif

Ingatlah dari bab sebelumnya bahwa auditor menghubungkan kekuatan dan kelemahan dalam pengendalian internal ke sasaran hasil audit yang terkait dengan transaksi yang spesifik. Berdasarkan pada kekuatan dan kelemahan itu, auditor menilai risiko pengendalian untuk masing-masing sasaran audit yang terkait dengan transaksi. Pendekatan yang sama itu digunakan dalam lingkungan TI, tetapi sekarang auditor mungkin mampu percaya pada pengendalian aplikasi yang dilakukan oleh komputer untuk mengurangi risiko pengendalian.

Auditor biasanya tidak menghubungkan kekuatan dan kelemahan dalam pe- ngendalian umum ke sasaran hasil audit yang terkait dengan transaksi yang spesifik. Seperti lingkungan pengendalian, pengendalian umum mempengaruhi sasaran hasil audit yang terkait dengan transaksi dalam beberapa siklus. Jika pengendalian umum tidak efektif, kemampuan auditor untuk percaya pada pengendalian aplikasi untuk mengurangi risiko pengendalian telah dikurangi. Dan sebaliknya, jika pengendalian umum adalah efektif, itu meningkatkan kemampuan auditor untuk percaya pada pe- ngendalian aplikasi untuk mengurangi risiko kendali.

Auditor mengidentifikasikan baik pengendalian manual dan pengendalian aplikasi yang dilakukan komputer dan kelemahan untuk masing-masing sasaran audit yang terkait dengan transaksi yang menggunakan suatu matriks risiko pengendalian dalam cara yang hampir sama seperti yang dibahas dalam bab sebelumnya.

4.3. Mengaudit dalam Lingkungan TI yang Tidak Terlalu Rumit

Banyak organisasi menggunakan TI untuk memroses transaksi bisnis dan merancang sistem tersebut sedemikian sehingga dokumen sumber dapat diperoleh kembali dalam format yang dapat dibaca dan dengan mudah bisa ditelusuri melalui sistem akuntansi ke keluaran. Dalam kejadian itu, banyak dokumen sumber yang tradisional seperti pesanan pembelian pelanggan, arsip pengiriman dan penerimaan, dan faktur penjualan dan pemasok. Perangkat lunak akuntansi yang terkait juga menghasilkan jurnal dan buku besar tercetak yang mengijinkan auditor untuk melacak transaksi individu melalui arsip akuntansi. Sebagai tambahan, pengendalian internal sering meliputi perbandingan klien atas arsip yang dihasilkan-komputer dengan dokumen sumber.

Dalam situasi ini, penggunaan TI tidak terlalu berdampak pada jejak audit. Biasanya, auditor memperoleh suatu pemahaman dari pengendalian internal dan melaksanakan ujian dari pengendalian, ujian substantif transaksi, dan prosedur verifikasi saldo akun dengan cara yang sama seolah sistem akuntansi seluruhnya manual. Auditor masih bertanggung jawab untuk memperoleh suatu pemahaman dari pengen- dalian komputer umum dan aplikasi karena pengetahuan demikian bermanfaat dalam mengidentifikasikart risiko yang bisa mempengaruhi laporan keuangan. Namun, biasa- nya auditor tidak melaksanakan ujian pengendalian komputer. Pendekatan audit ini sering disebut mengaudit di sekitar komputer sebab auditor tidak menggunakan pengendalian komputer untuk mengurangi risiko pengendalian yang ditaksir.

4.4. Mengaudit dalam Lingkungan TI yang Lebih Rumit

Ketika organisasi memperluas penggunaan TI mereka, pengendalian internal sering ditanamkan di dalam aplikasi yang hanya terlihat dalam format elektronik. Ketika dokumen sumber yang tradisional seperti faktur, pesanan pembelian, arsip penagihan, dan arsip akuntansi seperti jurnal penjualan, daftar persediaan, dan

catatan tambahan piutang dagang adalah hanya dalam format elektronik dibandingkan dengan aslinya (hard copy), auditor harus mengubah pendekatan ke audit. Pendekatan kepada audit ini sering disebut mengaudit melalui komputer.

Ada tiga kategori dari pengujian strategi ketika mengaudit melalui komputer: pendekatan data ujian, simulasi paralel, dan pendekatan modul audit tertanam.

a. Pendekatan Data Ujian. Pendekatan data ujian melibatkan pengolahan data ujian auditor menggunakan sistem komputer klien dan program aplikasi klien untuk menentukan apakah pengendalian yang dilakukan-komputer dengan tepat memproses data ujian itu. Karena auditor merancang data ujian itu, auditor bisa mengidentifikasi- kan materi ujian mana yang harus diterima atau ditolak oleh sistem klien. Auditor mem- bandingkan keluaran yang dihasilkan oleh sistem dari ujian data kepada keluaran yang diharapkan untuk menilai efektivitas dari aplikasi pengendalian internal program.

   Ketika menggunakan pendekatan data ujian, ada tiga pertimbangan auditor yang utama:

   a) Data ujian harus meliputi semua kondisi relevan yang ingin diuji auditor. Auditor harus merancang data ujian untuk menguji pengendalian kunci berbasiskomputer yang cenderung dipercayai auditor untuk mengurangi risiko pengendalian.
   b) Program aplikasi yang diuji oleh data ujian auditor harus sama dengan yang digunakan klien sepanjang tahun. Satu pendekatan adalah untuk menjalankan data ujian atas dasar kejutan, mungkin secara acak sepanjang tahun, walaupun melakukannya adalah mahal dan meng- habiskan waktu.
   c) Data ujian harus dihapuskan dari arsip klien. Jika uji coba perangkat lunak klien melibatkan data ujian pemrosesan selagi secara serempak memroses transaksi klien sebenarnya, auditor harus mengbilangkan data ujian di dalam arsip induk klien ketika pengujian selesai.

b. Simulasi Paralel. Berbagai perangkat lunak telah tersedia untuk membantu auditor dalam menentukan efektivitas pengendalian dalam perangkat lunak dan untuk memperoleh bukti tentang saldo akun yang dalam suatu format

elektronik. Auditor rnenggunakan perangkat lunak yang dikontrol-auditor untuk melaksanakan operasional paralel kepada perangkat lunak klien dengan menggunakan arsip data yang sama. Ketiadaan perbedaan di dalam keluaran menunjukan perangkat lunak klien yang berfungsi secara efektif, sedangkan perbedaan menandai adanya kelemahan poten- sial. Sebab perangkat lunak auditor dirancang untuk memparalel suatu operasi yang dilakukan oleh perangkat lunak klien, strategi pengujian ini disebut pengujian simulasiparalel.

c. Pendekatan Modul Audit Tertanam. Saat menggunakan pendekatan modul audit tertanam, auditor memasukkan suatu modul audit dalam sistem aplikasi klien untuk menangkap transaksi dengan karakteristik yang menjadi minat spesifik auditor itu. Suatu keuntungan yang penting adalah kemampuan auditor menguji secara terus menerus, membandingkan dengan data ujian dan pendekatan simulasi paralel, yang dilaksanakan pada titik waktu tertentu. Keuntungan lain dari modul audit tertanam adalah kemampuan untuk mengidentifikasi semua transaksi yang tidak biasa untuk evaluasi auditor.

5. Masalah-Masalah Untuk Llngkungan TI Yang Berbeda

5.1. Masalah Untuk Lingkungan Komputer Mikro

Komputer mikro secara luas digunakan dalam banyak bisnis dengan mengabai- kan ukuran organisasi itu. Umumnya mereka memainkan suatu peran yang penting untuk bisnis yang kecil dalam memroses atau meneliti data akuntansi melalui penggunaan perangkat lunak akuntansi dan neraca lajur elektronik yang dibeli atau dibuat khusus.

Pengendalian umum dalam perusahaan yang lebih kecil pada umumnya sedikit kurang efektif dibanding dalam lingkungan TI yang lebih rumit. Seringkali, tidak ada IT personil yang khusus atau klien bersandar pada keterlibatan berkala konsultan TI untuk membantu dalam memasang dan memelihara perangkat keras dan lunak.

Seringkali, auditor dari klien yang menggunakan komputer mikro dalam lingkung- an pengendalian umum yang tidak terlalu canggih melakukan sebagian besar audit mereka di sekitar komputer. Sistem ini sering menghasilkan jejak audit yang memadai yang mengijinkan auditor untuk merekonsiliasikan dokumentasi sumber masukan untuk keluaran.

Namun, bahkan dalam lingkungan TI yang tidak terlalu canggih, ada situasi di mana bisa bersandar pada pengendalian komputer. Sebagai contoh, program perangkat lunak dalam komputer mikro dapat diisikan pada hard-drive komputer dalam format yang tidak mengijinkan perubahan oleh personil klien. Risiko dari perubahan yang tidak sah di perangkat lunak kemudian menjadi rendah. Sebelum bersandar pada pengendalian yang dibangun ke dalam perangkat lunak tersebut, auditor harus mempunyai kepercayaan pada reputasi penjual perangkat lunak untuk mutunya.

Risiko lain dengan komputer mikro adalah bilangnya data dan program oleh karena virus komputer, yang dapat menyebar ke program lain dan sistem keseluruhan. Virus tertentu dapat merusak disk arsip atau menutup keseluruhan jaringan komputer. Memperbarui perangkat lunak pelindung virus secara teratur yang secara terus menerus menyaring penyebaran virus meningkatkan pengendalian.

5.2. Masalah Lingkungan Jaringan

Penggunaan jaringan yang makin meledak yang menghubungkan peralatan seperti komputer mikro, komputer jangkauan menengah, mainframe, stasiun kerja, server, dan pencetak sedang mengubah fungsi TI untuk banyak bisnis. Jaringan area lokal (Local Area Network/LAN) menghubungkan peralatan di dalam lingkungan bangunan yang kecil atau tunggal dan hanya digunakan untuk tujuan intra perusahaan. Penggunaan umum LAN adalah untuk memindahkan data dan program dari satu komputer atau stasiun kerja ke yang lainnya untuk mengijinkan semua alat untuk berfungsi bersama-sama. Jaringan Area Luas (WIde Area Network/WAN) menghu- bungkan peralatan dalam daerah geografis yang lebih besar, termasuk operasional global.

Dalam lingkungan jaringan, perangkat lunak aplikasi dan arsip data digunakan untuk memroses transaksi yang berada pada server, yang merupakan alat untuk mengolah data. Akses ke aplikasi dari komputer mikro atau stasiun-kerja diatur oleh perangkat lunak server jaringan. Perusahaan seringkali mempunyai beberapa server.

Saat klien mempunyai aplikasi akuntansi yang diproses dalam lingkungan jaringan, pemahaman auditor akan pengendalian internal perlu meliputi pengetahuan konfi- gurasi jaringan, mencakup penempatan dan server, stasiun-kerja, dan

komputer yang dihubungkan satu sama lain, dan pengetahuan perangkat lunak jaringan yang diguna- kan untuk mengatur sistem. Auditor juga harus memahami tentang pengendalian atas akses dan perubahan kepada program aplikasi dan arsip data yang ditempatkan pada server.

6. Masalah Sistem Manajemen Database

Auditor sering menghadapi aplikasi akuntansi yang menggunakan sistem mana- jemen database untuk memroses transaksi dan memelihara arsip data. Sistem mana- jemen database mengijinkan klien untuk menciptakan database yang berisi informasi yang dapat digunakan bersama dalam berbagai aplikasi. Dalam lingkungan non- database, masing-masing aplikasi berisi arsip data mereka sendiri, sedangkan dalam sistem manajemen database, banyak aplikasi berbagi arsip. Klien menerapkan sistem manajemen database untuk mengurangi kelebihan data, meningkatkan pengendalian atas data, dan menyediakan informasi yang lebih baik untuk pengambilan keputusan dengan pengintegrasian informasi seluruh fungsi dan departemen. Sebagai contoh, data pelanggan, seperti alamat dan nama pelanggan, dapat digunakan bersama di fungsi penjualan, kredit, akuntansi, pemasaran, dan pengiriman, yang menghasilkan pengurangan biaya yang penting. Perusahaan sering mengintegrasikan sistem mana- jemen database ke seluruh organisasi. Program demikian disebut perangkat lunak perusahaan.

Kendali sering meningkat ketika data dipusatkan dalam sistem manajemen database dengan penghapusan arsip data yang berlebihan. Namun, sistem mana- jemen database juga dapat membuat risiko pengendalian internal. Sebagai contoh, ada risiko yang berhubungan dengan berbagai pemakai, mencakup individu di luar akuntansi, mengakses dan memperbarui arsip data. Tanpa administrasi database dan pengendalian akses yang tepat, risiko arsip data yang tidak sah, tidak akurat, dan tidak sempurna menjadi meningkat. Juga, pemusatan data ke dalam arsip tunggal mening- katkan pentingnya backup yang sesuai atas informasi data secara teratur.

Auditor dan klien yang menggunakan sistem manajemen database perlu mema- hami perencanaan klien, organisasi, dan kebijakan dan prosedur untuk menentukan seberapa baik sistem itu diatur.

7. Masalah Untuk Sistem E-commerce

Perusahaan yang menggunakan sistem e-commerce untuk melakukan transaksi bisnis secara elektronis menghubungkan sistem akuntansi internal mereka ke sistem yang dipelihara oleh pihak luar, seperti pelanggan dan pemasok. Sebagai hasilnya, risiko yang dihadapi suatu perusahaan saat terlibat dengan aktivitas e-commerce sebagian bergantung pada seberapa baik mitra e-commerce-nya mengidentifikasi dan mengatur risiko dalam sistem TI mereka sendiri. Untuk mengatur risiko interdepen- densi ini, perusahaan harus memastikan bahwa micra bisnis mereka secara efektif mengatur risiko sistem TI sebelum melaksanakan bisnis dengan mereka secara elektronis.

Penggunaan dari sistem e-commerce juga menyingkapkan data perusaha-an yang sensitip, program, dan perangkat keras terhadap pemotongan yang potensi atau sabotase oleh pihak luar. Untuk membatasi keterbukaan ini, perusahaan mengguna- kan firewalls, teknik pengkodean, dan tandatangan digital. Firewall melindungi data, program, dan sumber daya TI lain dari para pemakai eksternal yang mengakses sistem melalui jaringan, seperti Internet. Firewall adalah suatu sistem dari perangkat keras dan lunak yang mengawasi dan mengendalikan aliran komunikasi e-commerce dengan penyaluran semua hubungan jaringan melalui suatu pintu gerbang pengendalian. Firewall dapat digunakan untuk memverifikasi pemakai eksternal dari jaringan, mem- berikan akses yang sah, dan mengarahkan pemakai ke program atau data yang di- minta.

Perusahaan menggunakan teknik pengkodean untuk melindungi keamanan komunikasi elektronik sepanjang proses transmisi. Teknik pengkodean didasarkan pada program komputer yang mengubah suatu pesan standar ke dalam suatu bentuk kode (encrypted). Penerima dari pesan elektronik itu harus menggunakan suatu program dekripsi (decryption) untuk memecahkan kode pesan itu. Seringkali teknik pengkodean kunci publik digunakan dimana satu kunci (kunci publik) digunakan E untuk menyandi pesan dan kunci yang lain (kunci pribadi) digunakan untuk memecah- kan kode pesan itu. Kunci publik dibagikan kepada pemakai yang disetujui dari sistem e-commerce itu dan hanya dapat digunakan untuk menyandikan pesan. Kunci pribadi, yang digunakan untuk memecahkan kode pesan, menjadi titik utama dari pengendali- an. Perlindungan kunci pribadi sering menjadi tanggung jawab dan administrator keamanan TI dan hanya dibagikan ke para pemakai internal dengan otoritas untuk memecahkan kode pesan itu.

Untuk membantu membuktikan keaslian kebenaran mitra dagang yang melaksa- nakan bisnis secara elektronik, perusahaan boleh bersandar pada otoritas sertifikasi eksternal

yang memverifikasi sumber dari kunci publik melalui penggunaan tanda tangan digital. Suatu otoritas sertifikasi yang dipercaya mengeluarkan suatu sertifikat digital kepada individu dan perusahaan yang terlibat dalam e-commerce. Tanda tangan digital berisi nama pemilik dan kunci publiknya. Juga berisi nama dari otoritas sertifikasi dan tanggal tidak berlakunya sertifikat dan informasi khusus lainnya. Untuk menjamin keaslian dan integritas, masing-masing tandatangan secara digital ditandatangani oleh kunci pribadi yang dipelihara oleh otoritas sertifikasi.

8. Masalah Saat Klien Menggunakan Ti Pihak Luar

Banyak klien membuka beberapa atau semua kebutuhan TI mereka kepada pusat pelayanan komputer yang independen bukannya memelihara suatu pusat TI in- ternal. Banyak perusahaan yang lebih kecil membuka fungsi penggajian mereka ke pihak luar karena penggajian adalah cukup standar dari perusahaan ke perusahaan dan di sana ada penyedia jasa penggajian yang dapat dipercaya. Perusahaan juga membuka sistem e-commerce mereka ke penyedia jasa situs Web eksternal. Seperti semua keputusan menggunakan pihak luar, perusahaan memutuskan apakah akan menggunakan TI pihak luar atas dasar manfaat-biaya.

Ketika menggunakan pusat jasa komputer pihak luar, klien menyerahkan data masukan, yang diproses oleh pusat jasa untuk suatu pembayaran (fee), dan mengem- balikan keluaran yang telah disepakati dan masukan asli. Untuk penggajian, per- usahaan menyerahkan kartu catatan waktu, tingkat upah, dan W4 kepada pusat jasa. Pusat jasa mengembalikan cek pembayaran upah, jurnal, dan data masukan setiap minggu dan W-2 pada akhir tiap tahun. Pusat jasa bertanggung jawab atas peran- cangan sistem komputer dan menyediakan pengendalian yang memadai untuk memastikan bahwa pemrosesan dapat dipercaya.

Auditor menghadapi suatu kesukaran ketika memperoleh suatu pemahaman dari pengendalian internal klien sebab banyak pengendalian itu berada di pusat jasa dan auditor tidak bisa berasumsi bahwa pengendalian adalah memadai hanya karena pusat jasa adalah suatu perusahaan independen. Standar audit meminta auditor untuk mempertimbangkan kebutuhan untuk memahami dan menguji pengendalian pusat jasa jika aplikasi pusat jasa melibatkan pemrosesan data keuangan yang penting.

Tingkat memperoleh pemahaman dan pengujian pengendalian pusat jasa harus didasarkan pada kriteria yang sama yang diikuti auditor dalam mengevaluasi pengen- dalian internal

klien. Dalamnya pemahaman itu tergantung pada kompleksitas sistem dan tingkat dimana auditor berniat untuk menglirangi risiko pengendalian yang dinilai untuk mengurangi ujian audit substantif. Jika auditor menyimpulkan bahwa keterlibatan yang aktif dipusat jasa adalah satu-satunya cara melakukan audit, mungkin saja perlu untuk memperoleh suatu pemahaman akan pengendalian internal dipusat jasa dan menguji pengendalian menggunakan data ujian dan ujian pengendalian lainnya.

Dibeberapa tahun terakhir, makin menjadi umum untuk mempunyai auditor inde- penden memperoleh suatu pemahaman dan menguji pengengdalian internal dari pusat jasa untuk digunakan oleh semua pelanggan dan auditor independen mereka. Tujuan penilaian independen ini adalah untuk menyediakan pelanggan pusat jasa dengan suatu tingkat jaminan yang layak dari ketercukupan pengendalian umum dan aplikasi milik pusat jasa dan untuk menghapuskan kebutuhan akan audit yang berlebihan oleh auditor pelanggan. Jika pusat jasa mempunyai banyak pelanggan dan masing-masing memerlukan suatu pemahaman dari pengendalian internal pusat jasa oleh auditor inde-penden mereka sendiri, kerepotan dan biaya untuk pusat jasa itu bisa besar. Ketika auditor independen pusat jasa menyelesaikan pemahaman dan uji coba atas pengendalian pusat jasa, maka dikeluarkan suatu laporan khusus, yang menunjukan lingkup dari audit dan kesimpulannya. Kemudian akan menjadi tanggung jawab dari auditor pelanggan untuk memutuskan tingkat dari kepercayaan pada pusat jasa. SAS 70 (AU 324) seperti dikembangkan oleh SAS 78 dan SAS 88 berisi bimbingan baik untuk auditor pelanggan dan auditor pusat jasa.

Referensi

http://www.coso.org/documents/internal%20controlintegrated%20framework.pdf.

https://mihok.my.id/pengendalian-internal-berkaitan-dengan-it/

https://www.isaca.org/popup/Pages/ApplicationControls.aspx.

https://www.academia.edu/6530656/Auditing_-_TI

Nama : Adiktia
NIM : 182420101
Kelas : MTI.20.A
Mata Kuliah : IT Audit

PROSES CONTROL (PENGENDALIAN)

Fungsi Pengendalian/pengawasan merupakan suatu unsur manajemen untuk melihat apakah segala kegiatan yang dilaksanakan telah sesuai dengan rencana yang digariskan dan disamping itu merupakan hal yang penting pula untuk menentukan rencana kerja yang akan datang.

Konntzdan O'Donnell (1964), mengartikan bahwa pengendalian atau pengawasan adalah pengukuran atau perbaikan terhadap pelaksanaan kerja bawahan agar rencana-rencana yang telah dibuat untuk mencapai tujuan organisasi dapat terselenggara dengan baik. Dalam uraian tersebut menggambarkan bahwa pengendalian atau pengawasan dapat dirumuskan sebagai proses penentuan apa yang akan dicapai, yaitu standar apa yang sedang dilakukan berupa; pelaksanaan, dan bila mana perlu melakukan perbaikan-perbaikan, sehingga pelaksanaannya sesuai dengan rencana yang ditetapkan.

George R. Terry, menyatakan bahwa pengawasan adalah proses penentuan apa yang akan dicapai , yaitu standar, apa yang sedang dihasilkan, yaitu pelaksanaan, menilai pelaksanaan dan bila perlu mengambil tindakan korektif sehingga pelaksanaan dapat berjalan sesuai rencana, yaitu sesuai standar. Juga merumuskam pengendalian (controlling) sebagai suatu usaha untuk meneliti kegiatan-kegiatan yang telah akan dilaksanakan.

Menurut **Sukanto Reksohadiprodjo,** pengawasan pada hakikatnya merupakan usaha memberi petunjuk pada para pelaksana agar mereka selalu bertindak sesuai dengan rencana. Lebih lanjut dikatakan bahwa pengawasan terdiri dari penentuan-penentuan standar, supervise kegiatan atau pemeriksaan, pembandingan hasil dengan standar serta mengoreksi kegiatan atau standar.

Menurut **Winardi** (1990; 380) dalam bukunya Azas-azas Manajemen, dikatakan bahwa prinsip pengawasan efektif membantu usaha-usaha kita untuk mengatur pekerjaan yang direncanakan

untuk memastikan bahwa pelaksanaan pekerjaan tersebut berlangsung sesuai dengan rencana. Sementara itu **Harold Koontz dan Cyril O'Donnell** (1988; 558)mengemukakan Azas-azas/Prinsip-prinsip Pengendalian /pengawasan sebagai berikut :

a. Prinsip tercapainya tujuan (principle of assurance of objective),
   Pengendalian harus ditujukan ke arah tercapainya tujuan, yaitu dengan mengadakan perbaikan (koreksi) untuk menghindarkan penyimpangan/deviasi dari perencanaan.
b. Prinsip efisiensi pengendalian (principle of efesience of control)
   Pengendalian efisiensi ini bertujuan untuk menghindarkan deviasi-deviasi dari perencanaan sehingga tidak menimbulkan ha-hal lain yang diluar dugaan.
c. Prinsip tanggung jawab pengendalian (Principle of control responbility)
   Pengendalian hanya dapat dilaksanakan apabila managr dapat bertanggung jawab terhadap pelaksanaan rencana.
d. Prinsip pengendalian terhadap masa depan (principle of future control)
   Pengendalian yang efektif harus ditujukan ke arah pencegahan, penyimpangan, perencanaan yang akan terjadi, baik sekarang maupun pada masa yang akan datang.
e. Prinsip pengendalian langsung (principle of direct control)
   Tehnik control yang paling efektif adalah mengusahakan adanya bawahan yang berkualitas baik.
f. Prinsip refleksi perencanaan (principle of reflection of plan)
   Perencanaan harus disusun dengan baik, sehingga dapat mencerminkan karakter dan susunan perencanaan.
g. Prinsip penyesuaian dengan organisasi (principle of organizational)
   Pengendalian harus dilaksanakan sesuai dengan struktur organisasi. Manager dan bawahannya merupakan sasaran untuk melaksanakan rencana.
h. Prinsip pengendalian individual (principle of individually of control)
   Pengendalian dan tehnik pengendalian harus sesuai dengan kebutuhan manajer.
i. Prinsip standar (principle of standar)
   Control yang efektif dan efesien memerlukan standar yang tepat sebagai tolak ukur pelaksanaan dan tujuan yang akan dicapai.

Pengendalian dapat dilakukan melalui tahap-tahap yang telah ditentukan berdasarkan perencanaan yang telah disusun sebelumnya. Pendapat tentang pengendalian banyak dilakukan

oleh para ahli, antara lain menurut pendapat **Hasibuan** (1990; 225), proses pengendalian atau control dapat dilakukan melalui tahap-tahap sebagai berikut :

1. Menentukan standar-standar atau dasar untuk melakukan control;
2. Mengukur pelaksanaan kerja;
3. Membandingkan pelaksanaan dengan standar dan menentukan deviasi
4. Melakukan tindakan-tindakan perbaikan jika terdapat penyimpangan (deviasi) agar pelaksanaan dan tujuan sesuai dengan rencana.

TUGAS IT AUDIT

NAMA : AGUS SUMITRO

NIM : 182420126

KELAS : MTI 20.A

DOSEN : Dr Widya Cholil , S.Kom., M.I.T.

SOAL :

untuk proses control (pengendalian) ada tindakan yang perlu dilaksanakan, gunakan referensi yang ada untuk menjawap pertanyaan saya tertutama dalam hal pengembangan sistem, pemrogramaan dan operasional

JAWAB :

1. Tindakan pengendalian yang perlu dilaksanakan dalam hal pengembangan sistem :
   - mengenali masalah yang dihadapi (recognize the prolem),
   - merumuskan problem yang sesungguhnya (define the problem),
   - menetapkan tujuan / sasaran (Set system objectives),
   - identifikasi kendala / keterbatasan (Identify system constraint),
   - melakukan studi kelayakan (conduct a feasibility study);
   - mengamati faktur – faktur yang berpengaruh terhadap pencapaian tujuan,
   - mencakup kelayakan, menyiapkan proposal (Prepare a system study proposal) dan disetujui / tidaknya usulan (approce or disapprove the study project),
   - membangun mekanisme kontrol (establish a control mechinisme)

2. Tindakan pengendalian yang perlu dilaksanakan dalam hal pemrograman
   - Kapabilitas programmer
   - Pemisahan fungsi
   - Standar metode , kinerja dan dokumen.
   - Batasi kewenangan
   - Menyediakan log manual dan machine log
   - Reviu independent oleh konsultan atau uji silang secara berkala

3. Tindakan pengendalian yang perlu dilaksanakan dalam hal operasional
   - Menetapkan sasaran kualitas bagi fungsi sistem informasi
   - Memonitor pemenuhan terhadap standar kualitas sistem informasi
   - Memberikan pelatihan kepada personil sistem informasi

AGUS WIRANTO

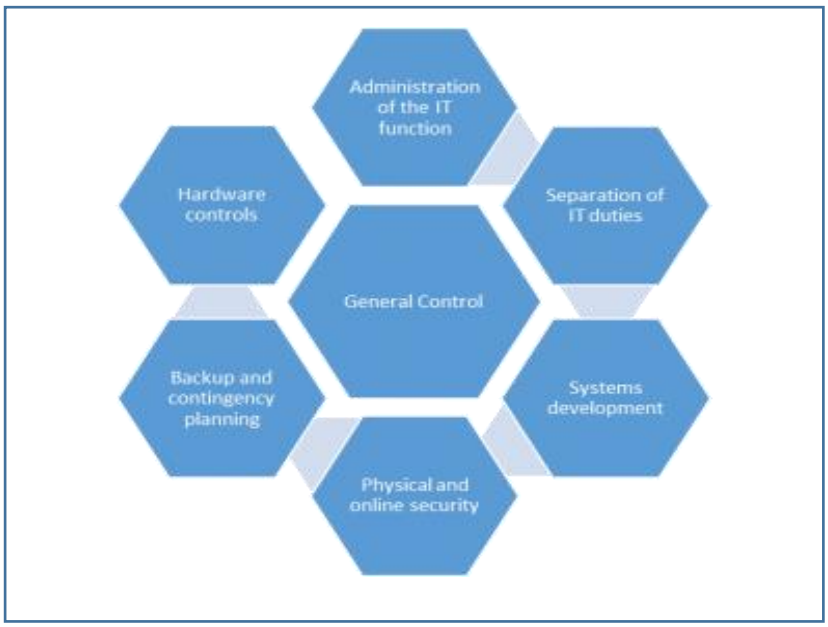
182420102 ➢ MTI2A1 ➢ IT Audit

➢ Control dan Audit TI

Ada dua jenis pengendalian yang berkaitan dengan pemanfaatan teknologi informasi yakni pengendalian umum (*general control/gen-con*) dan pengendalian aplikasi (*application control/app-con*). *General control* berkaitan dengan seluruh aspek dalam fungsi IT termasuk di dalamnya administrasi IT, pemisahan wewenang IT, pengembangan sistem, keamanan sistem informasi (secara fisik maupun dalam jaringan, atas *hardware*, *software* dan terlebih lagi data), backup dan perencanaan kontinjensi dalam keadaan darurat, serta pengendalian *hardware*. Pada umumnya *general-control* diterapkan pada skala entitas. Sedangkan *application control* diterapkan pada pemrosesan transaksi, misalnya pengendalian pada pemrosesan aktivitas penjualan dan penerimaan kas. Auditor diharuskan melakukan evaluasi pada *application control* atas kelas transaksi maupun akun yang hendak dikurangi risiko pengendaliannya. *Application control* hanya akan efektif bilamana *general control* efektif.

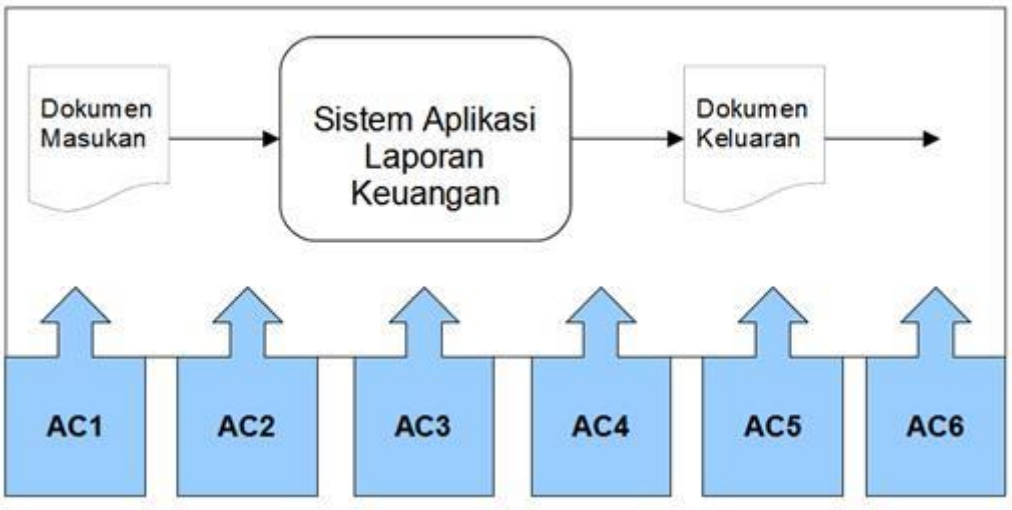
1. General Control

   Sebagaimana lingkungan pengendalian yang menjadi komponen dalam pengendalian internal menurut COSO[1], enam kategori dalam *general control* diterapkan dalam pengelolaan IT pada skala entitas. Dalam pelaksanaan audit, *general control* pada umumnya dievaluasi terlebih dahulu sebab pengaruhnya terhadap *application control*. Enam kategori dalam *general control* dijelaskan di bawah ini.



2. Application Control

ISACA[2] membagi *application control* ke dalam enam tahapan sebagaimana digambarkan pada diagram berikut ini.



Sumber: Modul 4 Training Information System Audit: Introduction to IT Governance and Management Standard – Tatakelola

AC1: *Source Data Preparation and Authorization*

Memberikan kepastian bahwa dokumen dipersiapkan serta diotorisasi oleh personel yang berwenang dengan mengikuti prosedur yang telah ditetapkan, dengan memperhatikan adanya pemisahan kewenangan yang memadai berkaitan dengan originasi dan persetujuan atas dokumen-dokumen tersebut. Meminimalkan adanya kesalahan maupun kelalaian melalui desain formulir *input* yang baik. Mendeteksi adanya kesalahan dan ketidakwajaran sehingga hal-hal tersebut dapat dilaporkan serta diambil langkah korektif.

AC2: *Source Data Collection and Entry*

Menjamin bahwa proses *input* data dilaksanakan secara *timely* oleh staf yang berwenang dan *qualified.* Koreksi dan submisi ulang atas data yang diinput secara keliru harus dilakukan tanpa adanya *compromising* atas tingkat otorisasi transaksi yang semestinya sekalipun mencukupi untuk dilaksanakannya rekonstruksi, namun dokumen sumber yang asli mesti tetap dijaga dalam jagka waktu tertentu.

AC3: *Accuracy, Completeness and Authenticity Checks*

Memastikan bahwasannya transaksi akurat, lengkap dan valid. Validasi atas *input* data, serta perubahan (*edit*) maupun pengiriman ulang oleh sebab adanya koreksi daam jangka waktu sependek mungkin dari *point of origination.*

AC4: *Processing Integrity and Validity*

Mempertahankan integritas serta validitas data sepanjang siklus pemrosesan. Pastikan bahwa deteksi atas transaksi yang keliru tidak mengganggu jalannya pemrosesan atas transaksi yang valid.

AC5: *Output Review, Reconciliation and Error Handling*

Menyelenggarakan prosedur-prosedur serta tanggung jawab terkait untuk memberikan kepastian bahwa *output* ditangani sesuai otorisasi yang diberlakukan, dikirimkan kepada penerima yang seharusnya serta diproteksi selama transmisi. Serta bahwa verifikasi, deteksi dan koreki atas akurasi input telah berjalan. Dan bahwasannya informasi yang disediakan dalam *output* seluruhnya dipergunakan.

AC6: *Transaction Authentication and Integrity*

Sebelum melewatkan data transaksi antar aplikasi internal dan fungsi bisnis atau operasional (ke dalam maupun ke luar *enterprise*), lakukan pengecekan atas *proper addressing*, otentisitas atas asal dan integritas konten. Pertahankan otentisitas dan integritas selama transmisi dan transpor.

Value and Risk Drivers for Application Control

Application Control	Value Drivers	Risk Drivers
	· Integritas data	· Adanya *compromised integrity* atas data kritikal
AC1: Source Data Preparation and Authorization	· Dokumentasi transaksi yang terstandarisasi dan diotorisasi · Kinerja aplikasi yang memadai · Akurasi data transaksi	· Transaksi-transaksi yang tidak diotorisasi maupun salah (*erroneous*) · Inefisiensi dalam pemrosesan maupun adanya pekerjaan berulang · Inefisiensi pemrosesan disebabkan oleh entri data yang tidak lengkap
AC2: Source Data Collection and Entry	• Entri data secara akurat dan pemrosesan secara efisien • Kesalahan terdeteksi secara *timely* · Pengamanan atas transaksi data yang sensitif	· Adanya *compromised integrity* atas data kritikal · Pelanggaran atas pengendalian hak akses · Kesalahan dalam entri data tidak terdeteksi

AC3: Accuracy, Completeness and Authenticity Checks	• Keslahan dalam pemrosesan data terremediasi secara efisien • Akurasi, kelengkapan serta validitas data terjaga selama pemrosesan • Tidak adanya interupsi dalam pemrosesan transaksi • Pemisahan wewenang untuk entri dan pemrosesan data	• Inefisiensi dalam pemrosesan maupun adanya pekerjaan berulang disebabkan oleh entri data yang tidak lengkap, tidak valid, maupun tidak akurat • Adanya *compromised integrity* atas data kritikal • Kesalahan dalam entri data tidak terdeteksi • Entri data yang tidak terotorisasi
AC4: Processing Integrity and Validity	• Melakukan pemrossan atas kesalahan yang terdeteksi secara *timely* • Kemampuan dalam melakukan investigasi permasalahan • Data *output* yang sensitif diproteksi	• Ketidakcukupan bukti atas terjadinya kesalahan maupun penyalahgunaan • Kesalahan dalam entri data yang tidak terdeteksi • Pemrosesan data yang tidak terotorisasi • Data transaksi yang sensitif dikirimkan pada penerima yang tidak semestinya
AC5: Output Review, Reconciliation and Error Handling	• Hasil pemrosesan yang lengkap serta bebas dari kesalahan dikirimkan kepada penerima yang berhak • Kesalahan terdeteksi secara *timely*	• Kerahasiaan data terlanggar (*compromised*) • Inefisiensi dalam pemrosesan transaksi • Kesalahan dalam *output* data transaksi tidak terdeteksi
AC6: Transaction Authentication and Integrity	• Straight-through processing • Confidence in validity and authenticity of transactions • Errors and misuse prevented	• Erroneous and/or unauthorized transactions • Transaction errors undetected • Inefficiencies and rework

1. TI Dalam peningkatan Pengendalian Internal

Kebanyakan entitas, termasuk bisnis kecil yng dimiliki keluarga berdasar pada TI untuk mencatat dan memproses transaksi bisnis. Sebagai hasil kemajuan luar biasa dalam di dalam TI, bahkan bisnis yang relatif sederhana menggunakan komputer pribadi dengan perangkat lunak akuntansi yang dibeli untuk proses akuntansi mereka. Penggunaan lingkungan jaringan yang kompleks, internet dn fungsi TI terpusat adalah umum dalam bisnis saat ini. Beberapa perubahan pengendalian internal yang diakibatkan oleh pengintegerasian TI ke dalam sistem akuntansi :

a. Kendali komputer menggantikan kendali manual.

Mamfaat yang nyata dari TI, seperti kemampuan untuk menangani volume yang luar biasa dari transaksi bisnis yang rumit secara hemat biaya, menyebabkan organisasi untuk menggunakan TI sepanjang proses pelaporan keuangan mereka. Satu keuntungan TI adalah kemampuan untuk meningkatkan pengendalian internal dengan menggabungkan kendali yang dilakukan komputer dalam aktivitas proses transaksi sehari-hari. Menggantikan prosedur manual dengan pengendalian yang diprogramkan yang menggunakan cek dan saldo bagi masing-masing transaksi yang diproses dapat mengurangi kesalahan manusia yang mungkin terjadi dalam lingkungan manual yang tradisional. Suatu sistem TI yang terkendali menawarkan potensi lebih besar untuk mengurangi salah saji karena komputer memroses informasi secara konsisten. Contoh dari pengendalian internal yang dilakukan oleh komputer yang pernah diproses oleh karyawan sedang membandingkan pelanggan dan nomor produk dengan arsip induk dan membandingkan jumlah transaksi penjualan dengan batas kredit yang telah diprogram. Pengendalian keamanan online dalam aplikasi, data-base, dan sistem operasional juga menyediakan peluang untuk meningkatkan pemisahan dari kewajiban.

b. Tersedianya informasi dengan mutu lebih tinggi.

Sekali manajemen yakin tentang keandalan informasi yang dihasilkan oleh TI, penggunaan manajemen atas informasi itu menawarkan potensi lebih lanjut untuk meningkatkan keputusan manajemen. Pertama-tama, lingkungan TI yang kompleks umumnya diatur secara efektif karena kompleksitas memerlukan organisasi yang efektif, prosedur, dan dokumentasi. Kedua, sistem TI biasanya menyediakan bagi manajemen lebih banyak informasi dengan mutu lebih tinggi dengan lebih cepat dari kebanyakan sistem manual.

2. Resiko yang Muncul dari Penggunaan Sistem Akuntansi Berbasis TI

Meskipun IT meningkatkan pengendalian intern perusahaan, hal ini juga dapat mempengaruhi resiko-resiko pengendalian perusahaan secara keseluruhan. resiko khusus pada sistem TI yaitu:

1) Resiko pada perngkat keras

Meskipun IT memberikan manfaat pemrosesan yang signifikan, hal itu juga menciptakan resiko yang unik dalam melindungi perangkat keras dan data, termasuk potensi munculnya jenis kesalahan baru. Resiko khusus ini mencakup hal-hal berikut:

a. Ketergantungan pada kemampuan berfungsinya perangkat keras dan lunak.
b. Kesalahan sistematis versus kesalahan acak
c. Akses yang tidak sah salah
d. Hilangnya data

2) Jejak audit yang berkurang

Salah saji mungkin tidak terdeteksi dengan meningkatnya penggunaan IT akibat hilangnya jejak audit secara nyata , termasuk berkurangnya keterlibatan manusia. selain itu, computer juga menggantikan jenis otorisasi tradisional dalam banyak sistem IT.

a. Visibilitas jejak audit. karena sebagian besar informasi dimasukan secara langsung ke dalam computer, penggunaan IT sering kali mengurangi atau bahkan meniadakan dokumen dan catatan sumber yang memungkinkan organisasi menelusuri informasi akuntansi.
b. Keterlibatan Manusia yang berkurang. Dalam banyak sistem IT, karyawan yang terlibat dengan pemrosesan awal transaksi tidak pernah melihat hasil akhirnya. Karena itu, mereka kurang mampu mengidentifikasi salah saji pemrosessan, Walapun mereka melihat outout akhir, sering kali sulit untuk mengenali salah saji karena hasilnya sering sangat ringkas.
c. Tidak adanya otorisasi traditiona. Sistem IT yang sangat canggih biasanya diprakarsai jenis transaksi tertentu secara otomatis, seperti perhitungan bunga atas rekening tabungan bank dan pemesanan persediaan apabila tingkat pesanan yang dtentukan telah dicapai,

3) Kebutuhan IT akan pengalaman dan pemisahan tugas

Sistem IT mengurangi sistem pemisahan tugas traditional (otorisasi, pembukuan, penyimpanan) dan menciptakan kebutuhan akan pengalaman IT tambahan.

3. Pengendalian Khusus atas Teknologi Informasi

Untuk menunjuk banyak dari risiko yang berhubungan dengan kepercayaan lebih besar atas TI, organisasi sering mengimplementasikan pengendalian khusus untuk fungsi TI. Standar audit menjelaskan dua pengelompokan pengendalian yang utama untuk sistem TI: pengendalian umum dan pengendalian aplikasi.

1) Pengendalian Umum (*General Control*), merupakan sistem pengendalian internal komputer yang berlaku umum dimana kegiatannya meliputi seluruh kegiatan komputerisasi sebuah perusahaan secara menyeluruh.

Auditor biasanya mengevaluasi pengendalian umum diawal audit oleh karena dampak dari pengendalian umum atas pengendalian aplikasi. Keenam kategori dari pengendalian umum kini diuji secara lebih detail. Keenam kategori tersebut adalah :

a. Administrasi dari Fungsi TI.
b. Pemisahan Tugas-tugas TI.
c. Pengembangan sistem.
d. Kemanan fisik dan online.
e. Backup dan Perencanaan Kontijensi
f. Pengendalian Perangkat Keras.

2) **Pengendalian Aplikasi** (*Application Control*), merupakan sistem pengendalian internal (*internal Controls*) pada sistem informasi berbasis teknologi informasi yang berkaitan dengan pekerjaan / kegiatan /aplikasi tertentu diamana setiap aplikasi mempunyai karakteristik tertentu dan kebutuhan pengendalian yang berbeda.

Pengendalian aplikasi dirancang untuk masing-masing aplikasi perangkat lunak dan dimaksudkan untuk membantu sebuah perusahaan memenuhi enam sasaran hasil audit yang terkait dengan transaksi. Walaupun beberapa pengendalian aplikasi mem-pengaruhi satu atau hanya beberapa sasaran hasil audit yang terkait dengan transaksi, kebanyakan kendali mencegah atau mendeteksi beberapa jenis salah saji.

Pengendalian aplikasi bisa dilakukan oleh komputer atau oleh manusia. Pengen-dalian aplikasi yang dilakukan oleh manusia yang berinteraksi dengan komputer sering dikenal sebagai pengendalian pemakai. Efektivitas dari pengendalian pemakai, seperti tinjauan ulang dari laporan pengecualian yang dihasilkan-komputer, sering tergantung pada akurasi dari informasi yang dihasilkan. Pengendalian aplikasi terdiri dari tiga kategori, yaitu :

1. Pengendalian input
2. Pengendalian Pemrosesan
3. Pengendalian output

Pengendalian umum di-rancang untuk melindungi semua pengendalian aplikasi untuk memastikan bahwa pengendalian itu efektif. Pengendalian umum yang kuat mengurangi jenis risiko yang dikenali di kotak di luar bentuk oval pengendalian umum.

4. Dampak Teknologi Informasi Pada Proses Audit

Auditor harus memiliki banyak pengetahuan tentang pengendalian ini sebab mereka bertanggung jawab atas perolehan suatu pemahaman dari pengendalian internal, termasuk pengendalian umum dan pengendalian aplikasi, dengan mengabaik- an apakah penggunaan TI oleh klien adalah kompleks atau sederhana. Juga, pe- ngetahuan tentang pengendalian umum meningkatkan kemampuan auditor untuk ber- sandar pada pengendalian aplikasi efektif untuk mengurangi risiko pengendalian untuk sasaran hasil audit yang terkait dengan transaksi.

1) Pengaruh dari Pengendalian Umum oleh Risiko Pengendalian

Kebanyakan auditor mengevaluasi efektivitas dari pengendalian umum sebelum mengevaluasi pengendalian aplikasi. Jika pengendalian umumnya tidak efektif, ada potensi untuk salah saji material pada setiap aplikasi akuntansi yang berbasis kompu- ter, dengan mengabaikan mutu dari pengendalian aplikasi.

Auditor biasanya memperoleh informasi tentang pengendalian umum dan aplikasi melalui wawancara dengan personil TI dan para pemakai kunci; pengujian dokumentasi sistem seperti bagan alur, manual pemakai, permohonan perubahan program, dan hasil pengujian; dan tinjauan ulang dari daftar pertanyaan terperinci yang diselesaikan oleh staf TI. Dalam banyak kasus, diinginkan untuk menggunakan beberapa pendekatan dalam pemahaman pengendalian internal karena masingmasing menawarkan informasi yang berbeda. Wawancara dengan pejabat kepala informasi dan analis sistem menyediakan informasi yang bermanfaat tentang pengoperasian keseluruhan fungsi TI, tingkat dari pengembangan perangkat lunak dan perangkat keras yang dibuat untuk perangkat lunak aplikasi akuntansi kunci, dan suatu ikhtisar dari perubahan yang direncanakan. Tinjauan ulang dari program mengubah per- mintaan dan hasil percobaan sistem adalah bermanfaat dalam mengidentifikasikan perubahan program dalam

perangkat lunak aplikasi. Daftar Pertanyaan berguna untuk mengidentifikasikan pengendalian internal yang spesifik.

2) Efek dari Pengendalian TI atas Risiko Pengendalian dan Ujian Substantif

Ingatlah dari bab sebelumnya bahwa auditor menghubungkan kekuatan dan kelemahan dalam pengendalian internal ke sasaran hasil audit yang terkait dengan transaksi yang spesifik. Berdasarkan pada kekuatan dan kelemahan itu, auditor menilai risiko pengendalian untuk masing-masing sasaran audit yang terkait dengan transaksi. Pendekatan yang sama itu digunakan dalam lingkungan TI, tetapi sekarang auditor mungkin mampu percaya pada pengendalian aplikasi yang dilakukan oleh komputer untuk mengurangi risiko pengendalian.

Auditor biasanya tidak menghubungkan kekuatan dan kelemahan dalam pe- ngendalian umum ke sasaran hasil audit yang terkait dengan transaksi yang spesifik. Seperti lingkungan pengendalian, pengendalian umum mempengaruhi sasaran hasil audit yang terkait dengan transaksi dalam beberapa siklus. Jika pengendalian umum tidak efektif, kemampuan auditor untuk percaya pada pengendalian aplikasi untuk mengurangi risiko pengendalian telah dikurangi. Dan sebaliknya, jika pengendalian umum adalah efektif, itu meningkatkan kemampuan auditor untuk percaya pada pe- ngendalian aplikasi untuk mengurangi risiko kendali.

Auditor mengidentifikasikan baik pengendalian manual dan pengendalian aplikasi yang dilakukan komputer dan kelemahan untuk masing-masing sasaran audit yang terkait dengan transaksi yang menggunakan suatu matriks risiko pengendalian dalam cara yang hampir sama seperti yang dibahas dalam bab sebelumnya.

3) Mengaudit dalam Lingkungan TI yang Tidak Terlalu Rumit

Banyak organisasi menggunakan TI untuk memroses transaksi bisnis dan merancang sistem tersebut sedemikian sehingga dokumen sumber dapat diperoleh kembali dalam format yang dapat dibaca dan dengan mudah bisa ditelusuri melalui sistem akuntansi ke keluaran. Dalam kejadian itu, banyak dokumen sumber yang tradisional seperti pesanan pembelian pelanggan, arsip pengiriman dan penerimaan, dan faktur penjualan dan pemasok. Perangkat lunak akuntansi yang terkait juga menghasilkan jurnal dan

buku besar tercetak yang mengijinkan auditor untuk melacak transaksi individu melalui arsip akuntansi. Sebagai tambahan, pengendalian internal sering meliputi perbandingan klien atas arsip yang dihasilkan-komputer dengan dokumen sumber.

Dalam situasi ini, penggunaan TI tidak terlalu berdampak pada jejak audit. Biasa- nya, auditor memperoleh suatu pemahaman dari pengendalian internal dan melak- sanakan ujian dari pengendalian, ujian substantif transaksi, dan prosedur verifikasi saldo akun dengan cara yang sama seolah sistem akuntansi seluruhnya manual. Auditor masih bertanggung jawab untuk memperoleh suatu pemahaman dari pengen- dalian komputer umum dan aplikasi karena pengetahuan demikian bermanfaat dalam mengidentifikasikart risiko yang bisa mempengaruhi laporan keuangan. Namun, biasa- nya auditor tidak melaksanakan ujian pengendalian komputer. Pendekatan audit ini sering disebut mengaudit di sekitar komputer sebab auditor tidak menggunakan pengendalian komputer untuk mengurangi risiko pengendalian yang ditaksir.

4) Mengaudit dalam Lingkungan TI yang Lebih Rumit

Ketika organisasi memperluas penggunaan TI mereka, pengendalian internal sering ditanamkan di dalam aplikasi yang hanya terlihat dalam format elektronik. Ketika dokumen sumber yang tradisional seperti faktur, pesanan pembelian, arsip penagihan, dan arsip akuntansi seperti jurnal penjualan, daftar persediaan, dan catatan tambahan piutang dagang adalah hanya dalam format elektronik dibandingkan dengan aslinya (hard copy), auditor harus mengubah pendekatan ke audit. Pendekatan kepada audit ini sering disebut mengaudit melalui komputer.

Ada tiga kategori dari pengujian strategi ketika mengaudit melalui komputer: pendekatan data ujian, simulasi paralel, dan pendekatan modul audit tertanam.

a. Pendekatan Data Ujian. Pendekatan data ujian melibatkan pengolahan data ujian auditor menggunakan sistem komputer klien dan program aplikasi klien untuk menentukan apakah pengendalian yang dilakukan-komputer dengan tepat memproses data ujian itu. Karena auditor merancang data ujian itu, auditor bisa mengidentifikasi- kan materi ujian mana yang harus diterima atau ditolak oleh sistem klien. Auditor mem- bandingkan keluaran yang dihasilkan oleh sistem dari

ujian data kepada keluaran yang diharapkan untuk menilai efektivitas dari aplikasi pengendalian internal program.

Ketika menggunakan pendekatan data ujian, ada tiga pertimbangan auditor yang utama:

a) Data ujian harus meliputi semua kondisi relevan yang ingin diuji auditor. Auditor harus merancang data ujian untuk menguji pengendalian kunci berbasiskomputer yang cenderung dipercayai auditor untuk mengurangi risiko pengendalian.
b) Program aplikasi yang diuji oleh data ujian auditor harus sama dengan yang digunakan klien sepanjang tahun. Satu pendekatan adalah untuk menjalankan data ujian atas dasar kejutan, mungkin secara acak sepanjang tahun, walaupun melakukannya adalah mahal dan meng- habiskan waktu.
c) Data ujian harus dihapuskan dari arsip klien. Jika uji coba perangkat lunak klien melibatkan data ujian pemrosesan selagi secara serempak memroses transaksi klien sebenarnya, auditor harus mengbilangkan data ujian di dalam arsip induk klien ketika pengujian selesai.

b. Simulasi Paralel. Berbagai perangkat lunak telah tersedia untuk membantu auditor dalam menentukan efektivitas pengendalian dalam perangkat lunak dan untuk memperoleh bukti tentang saldo akun yang dalam suatu format elektronik. Auditor rnenggunakan perangkat lunak yang dikontrol-auditor untuk melaksanakan operasional paralel kepada perangkat lunak klien dengan menggunakan arsip data yang sama. Ketiadaan perbedaan di dalam keluaran menunjukan perangkat lunak klien yang berfungsi secara efektif, sedangkan perbedaan menandai adanya kelemahan poten- sial. Sebab perangkat lunak auditor dirancang untuk memparalel suatu operasi yang dilakukan oleh perangkat lunak klien, strategi pengujian ini disebut pengujian simulasiparalel.
c. Pendekatan Modul Audit Tertanam. Saat menggunakan pendekatan modul audit tertanam, auditor memasukkan suatu modul audit dalam sistem aplikasi klien untuk menangkap transaksi dengan karakteristik yang menjadi minat spesifik auditor itu. Suatu keuntungan yang penting adalah kemampuan auditor menguji secara terus menerus, membandingkan dengan data ujian dan pendekatan simulasi paralel, yang dilaksanakan pada titik waktu tertentu. Keuntungan lain dari modul audit tertanam

adalah kemampuan untuk mengidentifikasi semua transaksi yang tidak biasa untuk evaluasi auditor.

5. Masalah-Masalah Untuk Llngkungan TI Yang Berbeda

1) Masalah Untuk Lingkungan Komputer Mikro

Komputer mikro secara luas digunakan dalam banyak bisnis dengan mengabai-kan ukuran organisasi itu. Umumnya mereka memainkan suatu peran yang penting untuk bisnis yang kecil dalam memroses atau meneliti data akuntansi melalui penggunaan perangkat lunak akuntansi dan neraca lajur elektronik yang dibeli atau dibuat khusus.

Pengendalian umum dalam perusahaan yang lebih kecil pada umumnya sedikit kurang efektif dibanding dalam lingkungan TI yang lebih rumit. Seringkali, tidak ada IT personil yang khusus atau klien bersandar pada keterlibatan berkala konsultan TI untuk membantu dalam memasang dan memelihara perangkat keras dan lunak. Seringkali, auditor dari klien yang menggunakan komputer mikro dalam lingkung- an pengendalian umum yang tidak terlalu canggih melakukan sebagian besar audit mereka di sekitar komputer. Sistem ini sering menghasilkan jejak audit yang memadai yang mengijinkan auditor untuk merekonsiliasikan dokumentasi sumber masukan untuk keluaran.

Namun, bahkan dalam lingkungan TI yang tidak terlalu canggih, ada situasi di mana bisa bersandar pada pengendalian komputer. Sebagai contoh, program perangkat lunak dalam komputer mikro dapat diisikan pada hard-drive komputer dalam format yang tidak mengijinkan perubahan oleh personil klien. Risiko dari perubahan yang tidak sah di perangkat lunak kemudian menjadi rendah. Sebelum bersandar pada pengendalian yang dibangun ke dalam perangkat lunak tersebut, auditor harus mempunyai kepercayaan pada reputasi penjual perangkat lunak untuk mutunya.

Risiko lain dengan komputer mikro adalah bilangnya data dan program oleh karena virus komputer, yang dapat menyebar ke program lain dan sistem keseluruhan. Virus tertentu dapat merusak disk arsip atau menutup keseluruhan jaringan komputer. Memperbarui perangkat lunak pelindung virus secara teratur yang secara terus menerus menyaring penyebaran virus meningkatkan pengendalian.

2) Masalah Lingkungan Jaringan

Penggunaan jaringan yang makin meledak yang menghubungkan peralatan seperti komputer mikro, komputer jangkauan menengah, mainframe, stasiun kerja, server, dan pencetak sedang mengubah fungsi TI untuk banyak bisnis. Jaringan area lokal (Local Area Network/LAN) menghubungkan peralatan di dalam lingkungan bangunan yang kecil atau tunggal dan hanya digunakan untuk tujuan intra perusahaan. Penggunaan umum LAN adalah untuk memindahkan data dan program dari satu komputer atau stasiun kerja ke yang lainnya untuk mengijinkan semua alat untuk berfungsi bersama-sama. Jaringan Area Luas (WIde Area Network/WAN) menghubungkan peralatan dalam daerah geografis yang lebih besar, termasuk operasional global.

Dalam lingkungan jaringan, perangkat lunak aplikasi dan arsip data digunakan untuk memroses transaksi yang berada pada server, yang merupakan alat untuk mengolah data. Akses ke aplikasi dari komputer mikro atau stasiun-kerja diatur oleh perangkat lunak server jaringan. Perusahaan seringkali mempunyai beberapa server.

Saat klien mempunyai aplikasi akuntansi yang diproses dalam lingkungan jaring- an, pemahaman auditor akan pengendalian internal perlu meliputi pengetahuan konfi- gurasi jaringan, mencakup penempatan dan server, stasiun-kerja, dan komputer yang dihubungkan satu sama lain, dan pengetahuan perangkat lunak jaringan yang diguna- kan untuk mengatur sistem. Auditor juga harus memahami tentang pengendalian atas akses dan perubahan kepada program aplikasi dan arsip data yang ditempatkan pada server.

3) Masalah Sistem Manajemen Database

Auditor sering menghadapi aplikasi akuntansi yang menggunakan sistem manajemen database untuk memroses transaksi dan memelihara arsip data. Sistem manajemen database mengijinkan klien untuk menciptakan database yang berisi informasi yang dapat digunakan bersama dalam berbagai aplikasi. Dalam lingkungan non-database, masing-masing aplikasi berisi arsip data mereka sendiri, sedangkan dalam sistem manajemen database, banyak aplikasi berbagi arsip. Klien menerapkan sistem manajemen database untuk mengurangi kelebihan data, meningkatkan pengendalian atas data, dan menyediakan informasi yang lebih baik untuk pengambilan keputusan dengan pengintegrasian informasi seluruh fungsi dan departemen. Sebagai contoh, data pelanggan, seperti alamat dan nama pelanggan, dapat digunakan bersama di fungsi penjualan, kredit, akuntansi, pemasaran, dan pengiriman, yang menghasilkan pengurangan biaya yang penting. Perusahaan sering mengintegrasikan sistem mana-

jemen database ke seluruh organisasi. Program demikian disebut perangkat lunak perusahaan.

Kendali sering meningkat ketika data dipusatkan dalam sistem manajemen database dengan penghapusan arsip data yang berlebihan. Namun, sistem manajemen database juga dapat membuat risiko pengendalian internal. Sebagai contoh, ada risiko yang berhubungan dengan berbagai pemakai, mencakup individu di luar akuntansi, mengakses dan memperbarui arsip data. Tanpa administrasi database dan pengendalian akses yang tepat, risiko arsip data yang tidak sah, tidak akurat, dan tidak sempurna menjadi meningkat. Juga, pemusatan data ke dalam arsip tunggal meningkatkan pentingnya backup yang sesuai atas informasi data secara teratur.

Auditor dan klien yang menggunakan sistem manajemen database perlu memahami perencanaan klien, organisasi, dan kebijakan dan prosedur untuk menentukan seberapa baik sistem itu diatur.

4) Masalah Untuk Sistem E-commerce

Perusahaan yang menggunakan sistem e-commerce untuk melakukan transaksi bisnis secara elektronis menghubungkan sistem akuntansi internal mereka ke sistem yang dipelihara oleh pihak luar, seperti pelanggan dan pemasok. Sebagai hasilnya, risiko yang dihadapi suatu perusahaan saat terlibat dengan aktivitas e-commerce sebagian bergantung pada seberapa baik mitra e-commerce-nya mengidentifikasi dan mengatur risiko dalam sistem TI mereka sendiri. Untuk mengatur risiko interdependensi ini, perusahaan harus memastikan bahwa micra bisnis mereka secara efektif mengatur risiko sistem TI sebelum melaksanakan bisnis dengan mereka secara elektronis.

Penggunaan dari sistem e-commerce juga menyingkapkan data perusaha-an yang sensitip, program, dan perangkat keras terhadap pemotongan yang potensi atau sabotase oleh pihak luar. Untuk membatasi keterbukaan ini, perusahaan menggunakan firewalls, teknik pengkodean, dan tandatangan digital. Firewall melindungi data, program, dan sumber daya TI lain dari para pemakai eksternal yang mengakses sistem melalui jaringan, seperti Internet. Firewall adalah suatu sistem dari perangkat keras dan lunak yang mengawasi dan mengendalikan aliran komunikasi e-commerce dengan penyaluran semua hubungan jaringan melalui suatu pintu gerbang pengendalian. Firewall dapat digunakan untuk memverifikasi pemakai eksternal dari jaringan, mem- berikan akses yang sah, dan mengarahkan pemakai ke program atau data yang di- minta.

Perusahaan menggunakan teknik pengkodean untuk melindungi keamanan komunikasi elektronik sepanjang proses transmisi. Teknik pengkodean didasarkan pada program komputer yang mengubah suatu pesan standar ke dalam suatu bentuk kode (encrypted). Penerima dari pesan elektronik itu harus menggunakan suatu program dekripsi (decryption) untuk memecahkan kode pesan itu. Seringkali teknik pengkodean kunci publik digunakan dimana satu kunci (kunci publik) digunakan E untuk menyandi pesan dan kunci yang lain (kunci pribadi) digunakan untuk memecahkan kode pesan itu. Kunci publik dibagikan kepada pemakai yang disetujui dari sistem e-commerce itu dan hanya dapat digunakan untuk menyandikan pesan. Kunci pribadi, yang digunakan untuk memecahkan kode pesan, menjadi titik utama dari pengendalian. Perlindungan kunci pribadi sering menjadi tanggung jawab dan administrator keamanan TI dan hanya dibagikan ke para pemakai internal dengan otoritas untuk memecahkan kode pesan itu.

Untuk membantu membuktikan keaslian kebenaran mitra dagang yang melaksa- nakan bisnis secara elektronik, perusahaan boleh bersandar pada otoritas sertifikasi eksternal yang memverifikasi sumber dari kunci publik melalui penggunaan tanda tangan digital. Suatu otoritas sertifikasi yang dipercaya mengeluarkan suatu sertifikat digital kepada individu dan perusahaan yang terlibat dalam e-commerce. Tanda tangan digital berisi nama pemilik dan kunci publiknya. Juga berisi nama dari otoritas sertifikasi dan tanggal tidak berlakunya sertifikat dan informasi khusus lainnya. Untuk menjamin keaslian dan integritas, masing-masing tandatangan secara digital ditandatangani oleh kunci pribadi yang dipelihara oleh otoritas sertifikasi.

5) Masalah Saat Klien Menggunakan Ti Pihak Luar

Banyak klien membuka beberapa atau semua kebutuhan TI mereka kepada pusat pelayanan komputer yang independen bukannya memelihara suatu pusat TI internal. Banyak perusahaan yang lebih kecil membuka fungsi penggajian mereka ke pihak luar karena penggajian adalah cukup standar dari perusahaan ke perusahaan dan di sana ada penyedia jasa penggajian yang dapat dipercaya. Perusahaan juga membuka sistem e-commerce mereka ke penyedia jasa situs Web eksternal. Seperti semua keputusan menggunakan pihak luar, perusahaan memutuskan apakah akan menggunakan TI pihak luar atas dasar manfaat-biaya.

Ketika menggunakan pusat jasa komputer pihak luar, klien menyerahkan data masukan, yang diproses oleh pusat jasa untuk suatu pembayaran (fee), dan mengem-

balikan keluaran yang telah disepakati dan masukan asli. Untuk penggajian, perusahaan menyerahkan kartu catatan waktu, tingkat upah, dan W4 kepada pusat jasa. Pusat jasa mengembalikan cek pembayaran upah, jurnal, dan data masukan setiap minggu dan W-2 pada akhir tiap tahun. Pusat jasa bertanggung jawab atas perancangan sistem komputer dan menyediakan pengendalian yang memadai untuk memastikan bahwa pemrosesan dapat dipercaya.

Auditor menghadapi suatu kesukaran ketika memperoleh suatu pemahaman dari pengendalian internal klien sebab banyak pengendalian itu berada di pusat jasa dan auditor tidak bisa berasumsi bahwa pengendalian adalah memadai hanya karena pusat jasa adalah suatu perusahaan independen. Standar audit meminta auditor untuk mempertimbangkan kebutuhan untuk memahami dan menguji pengendalian pusat jasa jika aplikasi pusat jasa melibatkan pemrosesan data keuangan yang penting.

Tingkat memperoleh pemahaman dan pengujian pengendalian pusat jasa harus didasarkan pada kriteria yang sama yang diikuti auditor dalam mengevaluasi pengendalian internal klien. Dalamnya pemahaman itu tergantung pada kompleksitas sistem dan tingkat dimana auditor berniat untuk menglirangi risiko pengendalian yang dinilai untuk mengurangi ujian audit substantif. Jika auditor menyimpulkan bahwa keterlibatan yang aktif dipusat jasa adalah satu-satunya cara melakukan audit, mungkin saja perlu untuk memperoleh suatu pemahaman akan pengendalian internal dipusat jasa dan menguji pengendalian menggunakan data ujian dan ujian pengendalian lainnya.

Dibeberapa tahun terakhir, makin menjadi umum untuk mempunyai auditor inde- penden memperoleh suatu pemahaman dan menguji pengengdalian internal dari pusat jasa untuk digunakan oleh semua pelanggan dan auditor independen mereka. Tujuan penilaian independen ini adalah untuk menyediakan pelanggan pusat jasa dengan suatu tingkat jaminan yang layak dari ketercukupan pengendalian umum dan aplikasi milik pusat jasa dan untuk menghapuskan kebutuhan akan audit yang berlebihan oleh auditor pelanggan. Jika pusat jasa mempunyai banyak pelanggan dan masing-masing memerlukan suatu pemahaman dari pengendalian internal pusat jasa oleh auditor inde-penden mereka sendiri, kerepotan dan biaya untuk pusat jasa itu bisa besar. Ketika auditor independen pusat jasa menyelesaikan pemahaman dan uji coba atas pengendalian pusat jasa, maka dikeluarkan suatu laporan khusus, yang menunjukan lingkup dari audit dan kesimpulannya. Kemudian akan menjadi tanggung jawab dari auditor pelanggan untuk memutuskan tingkat dari kepercayaan pada pusat

jasa. SAS 70 (AU 324) seperti dikembangkan oleh SAS 78 dan SAS 88 berisi bimbingan baik untuk auditor pelanggan dan auditor pusat jasa.

- https://mihok.my.id/pengendalian-internal-berkaitan-dengan-it/
- Sumber:http://www.coso.org/documents/internal%20controlintegrated%20framework.pdf.
- Sumber: https://www.isaca.org/popup/Pages/ApplicationControls.aspx.
- https://www.academia.edu/6530656/Auditing_-_TI

Nama : Arie Ansyah
NIM : 182420117
Kelas : MTI 20A
Mata Kuliah : IT Audit (Control dan Audit TI)

Untuk proses control (pengendalian) ada tindakan yang perlu dilaksanakan, gunakan referensi yang ada untuk menjawap pertanyaan saya tertutama dalam hal pengembangan sistem, pemrogramaan dan operasional

Jawab :

A. Tindakan yang dilakukan dalam pengendalian manajemen pengembangan sistem antara lain :
    1. Perencanaan : Melakukan studi kelayakan dalam hal Teknologi, Operasional, Ekonomi dan Perilaku
    2. Analisa : Defenisi kebutuhan penguna
    3. Perancangan :
        - Desain system : a. Rancangan pemrosesan, b. Rancangan alur data dan informasi , c. Rancangan database, d. Rancangan tampilan antara muka, e. Rancangan logikal & phisikal dan f. Rancangan platform
        - Desain Reguest for Proposal (RFP) dan Metode Penilaian : a. Undangan kepada vendor, b. Seleksi vendor
    4. Pengembangan :
        - Pemrograman : Coding dan Compiling dengan Membagi modul kepada para programmer – Mengkoordinasikan kegiatan pemrograman – Mengatur jadwal pemrograman
        - Pembuatan Dokumen : Dokumentasi system dan Dokumentasi pengguna
        - Pengujian Pengembangan : Pengujian Unit dan Pengujian Integrasi
        - Pengujian Operasional : Pengujian Sistem – Pengujian Kinerja – Pengujian Dokumentasi – Pengujian Penerimaan
        - Implementasi : Migrasi dan Konversi; Operasioanl dan Pemeliharaan

B. Tindakan yang dilakukan dalam pengendalian manajemen pemrograman antara lain :

1. Planning : Teknik estimasi biaya
2. Design : Pendekatan desain berdasarkan Bahasa pemrograman
3. Coding : Tahapan Coding – Strategi Coding
4. Testing : Tahapan pengujian – Jenis Pengujian
5. Operation & Maintenance : Pemantauan kinerja – metode pemeliharaan

Pengendalian pemrograman dilakukan :

- Kapabilitas programmer
- Pemisahan fungsi
- Standar metode, kinerja dan dokumentasi
- Batasi kewenangan
- Sediakan log manual dan machine log
- Reviu independent oleh konsultan atau uji silang secara berkala

C. Tindakan yang dilakukan dalam pengendalian manajemen OPerasi antara lain :

- Computer Operation controls
  - Operation control : menentukan fungsi yang harus dilakukan oleh operator dan otomasi
  - Scheduling Control : Menentukan urutan dan jadwal pekerjaan dalam platform hardware atau software
  - Maintenance Controls : Menentukan bagaimana hardware dipelihara dalam urutan operasi
- Network Operation Control
  - LAN : Physical & Logical Barriers
  - WAN : Network Control Terminal (NCT)
- Data Preparation and Entry
  - Desain dokumen sumber
  - Penyimpanan dokumen sumber
  - Desain screen input
  - Desain area entri data

- Production Control
  - Penerimaan dan pengiriman input dan output
  - Penjadwalan Kerja
  - Kesepakatan tingkat layanan dengan pengguna
  - Harga Transfer
  - Akuisisi perlengkapan komputer
- File Library
  - Penyimpanan Media
  - Penggunaan media
  - Pemeliharaan dan penghacuran media
  - Lokasi Media
- Documentation and Program Library
  - Mengelola dokumentasi sistem
  - Mengelola persediaaan perangkat lunak
- Help Desk/Technical Support
  - Inventory, logging dan reporting
- Capacity Planning and Performance Monitoring
  - Apakah ada aktivitas yang tidak terotorisasi
  - Apakah kinerja sistem pada tingkatan yang dapat diterima
  - Kebutuhan perangkat keras dan perangkat lunak
- Management of Outsourced Operations
  - Evaluasi terus menerus atas kemampuan finasial vendor
  - Memastikan ketaatan kontrak
  - Memastikan secara terus menerus pengendalian yang memadai
  - Memelihara prosedur disaster recovery