PENGENDALIAN SISTEM INFORMASI BERDASARKAN KOMPUTER

DIANA RAHMAWATI

Pendahuluan

Perkembangan teknologi informasi mendorong perusahaan-perusahaan dalam menjalankan proses bisnisnya memanfaatkan teknologi informasi dan berbagi sistem informasi perusahaan dengan pihak eksternal yang berhubungan dengan perusahaan seperti vendor, pelanggan, pemegang saham dan lembaga pemerintah.

Implikasi dari hal tsb diatas menjadikan sistem informasi perusahaan rentan terhadap masalah dan mendorong perusahaan untuk meningkatkan sistem pengendalian internalnya.

Karena pentingnya jaminan/garansi atas sistem informasi, AICPA (*american institute of certified public accountans*) dan CICA (*canadian institute of chartered accountants*) memperkenalkan standar baru untuk menguji dan memverifikasi keandalan suatu sistem informasi yang disebut dengan ***Systrust***

Sistem Yang Andal

Terdapat 4 prinsip suatu sistem dikatakan andal (berdasarkan *sys trust*):

1. Ketersediaan (*availability*) : tersedia untuk dioperasikan dan digunakan
2. Keamanan (*security*) : terlindung dari baik akses fisik maupun akses logis yang tidak memiliki otorisasi
3. Dapat dipelihara (*maintainability*) : dapat diubah bila diperlukan tanpa mempengaruhi ketrersediaan, keamanan dan integritas sitem
4. Integritas (*integrity*) : pemrosesan bersifat lengkap, akurat, tepat waktu dan diotorisasi.

Pengendalian Untuk memenuhi Prinsip Keandalan

Terdapat tiga kategori pengendalian yaitu:

- Perencanaan Strategis dan penganggaran
  - Ancaman : SI tidak mendukung strategi bisnis, kurangnya penggunaan sumberdaya, kebutuhan informasi tidak dipenuhi atau tidak dapat ditanggung.
- Mengembangkan rencana keandalan sistem
  - Ancaman : Ketidakmampuan untuk memastikan keandalan sistem
- Dokumentasi
  - Ancaman : Desain, Operasi, tinjauan, Audit dan perubahan sistem yang tidak efektif.

Tabel 8-1
Ringkasan Pengendalian Umum Utama Keandalan

Kategori Pengendalian	Ancaman/Risiko	Pengendalian
Perencanaan Strategis dan Penganggaran	SI tidak mendukung strategi bisnis, kurangnya penggunaan sumber daya, kebutuhan informasi tidak dipenuhi atau tidak dapat ditanggung	Rencana strategis berlapis yang secara periodik dievaluasi, tim penelitian dan pengembangan untuk menilai dampak teknologi baru atas jalannya bisnis, anggaran untuk mendukung rencana strategis
Mengem-bangkan rencana keandalan sistem	Ketidakmampuan untuk memastikan keandalan sistem	Memberikan tanggung jawab perencanaan ke pihak manajemen puncak; secara terus-menerus meninjau dan memperbarui rencana; mengidentifikasi, mendokumen-tasikan, dan menguji kebutuhan, tujuan, kebijakan, dan standar keandalan pemakai; mengidentifikasi dan meninjau seluruh persyaratan hukum yang baru maupun yang telah diubah; mencatat permintaan pemakai atas perubahan; mendokumentasikan, menganalisis, dan melaporkan masalah dalam hal keandalan sistem; menetapkan tanggung jawab kepemilikan, pneyimpanan, akses, dan pemeliharaan atas sumber daya informasi; mengembangkan program kesadaran atas keamanan serta mengkomuni-kasikannya pada seluruh pegawai; meminta pegawai baru untuk menandatangani perjanjian keamanan; melaksanakan penilaian risiko atas seluruh perubahan dalam lingkungan sistem
Dokumentasi	Desain, operasi, tinjauan, audit, dan perubahan sistem yang tidak efektif	Dokumentasi administratif (standar dan prosedur untuk memproses, menganalisis, mendesain, memprogram, menangani file dan menyimpan data), dokumentasi sistem (input aplikasi, tahap pemrosesan, output, kesalahan penanganan), dokumentasi operasi (konfigurasi perlengkapan, program, file, susunan dan pelaksanaan prosedur, tindakan korektif)

Ketersediaan

- Ketersediaan
  - Meminimalkan waktu kegagalan sistem
    - Preventive maintenance
      - UPS (Uninterruptible Power Suply)
      - Batas toleransi kesalahan
    - Rencana Pemulihan dari Bencana
      - Meminimalkan gangguan , kerusakan dan kerugian.
      - Memberi cara alternatif memproses informasi untuk sementara waktu
      - Meneruskan jalannya operasi normal sesegera mungkin

Ketersediaan (Continued)

- Melatih dan memperkenalkan personil dengan operasi perusahaan secara darurat.
- Prioritas proses pemulihan
- Jaminan Asuransi
- Backup data and File Program
  - » Pengamanan Elektronis
  - » Konsep Grandfather-father-son
  - » Prosedur pengulangan
- Penugasan Khusus
- Fasilitas cadangan komputer dan telekomunikasi
- Uji dan Revisi Periodik
- Dokumentasi yang lengkap

Tabel 8-2
Ringkasan Pengendalian Utama atas Ketersediaan

Kategori Pengendalian	Ancaman/Risiko	Pengendalian
Meminimalkan waktu kegagalan sistem	Hilangnya tenaga listrik atau kegagalan sistem yang mengganggu operasi bisnis yang penting, kehilangan atau kerusakan data	Kebijakan dan prosedur untuk menangani kehilangan tenaga listrik, kesalahan, kehilangan atau kerusakan data, serta masalah lainnya; jaminan atas bencana dan gangguan bisnis; pemeliharaan untuk pencegahan secara teratur atas komponen utama; sistem tenaga listrik yang stabil; batas toleransi kesalahan
Rencana pemulihan dari bencana	Perpanjangan gangguan atas pemrosesan data serta operasi bisnis karena kebakaran, bencana alam, sabotase atau vandalisme	Tanggung jawab koordinator adalah mengimplementasikan rencana, menetapkan prioritas pemulihan, menugaskan tanggung jawab untuk kegiatan pemulihan, mendokumentasikan dan menguji rencana, secara terus-menerus meninjau dan merevisi rencana; penyimpanan jarak jauh data dan file cadangan (pengaman elektronik/electronic *vaulting*, konsep rekonstruksi bertingkat/*grandfather-father-son*), prosedur untuk pulih dari kerugian atau dari kehancuran file (pemeriksaan di tempat serta pengulangan), jaminan asuransi, komputer cadangan serta fasilitas komunikasi (perjanjian resiprokal, ruang cadangan dengan dan tanpa fasilitas komputer/*hot and cold sites*, duplikat *hardware*, *software* serta peralatan penyimpanan data)

Pemisahan tugas dalam fungsi sistem

- Ancaman dan Resiko
  - Penipuan Komputer
- Pengendalian dengan cara Otoritas dan tanggung jawab harus dengan jelas dibagi diantara fungsi – fungsi berikut :
  1. Systems administration
  2. Network management
  3. Security management
  4. Change management
  5. Users
  6. Systems analysis
  7. Programming
  8. Computer operations
  9. Information system library
  10. Data control

Pengendalian Atas akses secara Fisik

- Ancaman/Resiko
  - Kerusakan komputer dan file, akses yang tidak memiliki otorisasi kedata rahasia
- Pengendalian
  - Letakan komputer dalam ruang terkunci
  - Batasi akses ke personil yang memiliki otorisasis saja.
  - Meminta ID Pegawai
  - Meminta pengunjung untuk menandatangani daftar tamu ketika mereka masuk dan meninggkalkan lokasi
  - Gunakan sistem Alarm
  - Install Pengunci pada PC dan peralatan Lainnya.
  - Simpan komponen yang penting jauh dari bahan berbahaya.
  - Pasang detektor asap dan api serta pemadam api

Pengendalian atas akses secara Logis

- Ancaman/Resiko
  - Akses yang tidak memiliki otorisasi ke software sistem, program aplikasi serta sumber daya sistem lainnya.
- Pengendalian
  - passwords
  - physical possession identification
  - biometric identification
  - compatibility tests

Perlindungan atas PC dan Jaringan Klien/Server

- Ancaman/Resiko
  - Kerusakan file komputer dan perlengkapannya, akses yang tidak memiliki otorisasi ke data rahasia, pemakai yang tidak dikenali sistem pengamanan.
- Pengendalian :
  - Latih pemakai tentang pengendalian PC.
  - Batasi data yang disimpan dan didownload.
  - Kebijakan dan Prosedur yang baik
  - Buat cadangan hard drive secara teratur.
  - Enkripsi file atau beri file password.

Pengendalian Internet dan e-commerce

- Ancaman/resiko
  - Kerusakan file data dan perlengkapan akses yang tidak memiliki otorisasi kedata rahasia.
- Pengendalian
  - Password, Ekripsi, Verifikasi routing, Amplop elektronik, Software pendeteksi virus, Firewall, pembuatan jalur khusus, tolak akses pegawai ke Internet, dan server internet tidak terhubung dengan komputer lainnya diperusahaan.

Tabel 8-3
Ringkasan Pengendalian Pengamanan Utama

Kategori Pengendalian	Ancaman/Risiko	Pengendalian
Pemisahan tugas dalam fungsi sistem	Penipuan komputer	Bagi dengan jelas otoritas dan tanggung jawab di antara administrasi sistem, manajemen jaringan, manajemen pengamanan, manajemen perubahan, pemakai, analis sistem, programer, operator komputer, pengelola perpustakaan sistem informasi, serta kelompok pengendali data.
Pengendalian atas akses secara fisik	Kerusakan komputer dan file; akses yang tidak memiliki otorisasi ke data rahasia	Letakkan komputer dalam ruang terkunci; batasi akses ke personil yang memiliki otorisasi saja; buat jalan masuk yang terkunci dengan aman dan diawasi dengan baik; meminta ID pegawai; meminta pengunjung untuk menandatangani daftar tamu ketika mereka masuk dan meninggalkan lokasi; gunakan sistem alarm; batasi akses ke saluran telepon pribadi yang tidak terdeteksi, ke terminal dan PC yang memiliki otorisasi; instal pengunci pada PC dan peralatan komputer lainnya; batasi akses ke program *off-line*, data serta perlengkapannya; simpan komponen sistem yang penting jauh dari bahan berbahaya; pasang detektor asap dan api serta pemadam api.
Pengendalian atas akses secara logis	Akses yang tidak memiliki otorisasi ke software sistem, program aplikasi, serta sumber daya sistem lainnya	Klasifikasi pengamanan data (tidak ada batasan, hanya untuk pegawai, hanya untuk pemilik dan manajemen puncak, dan lain-lain), tetapkan hak akses pegawai dan pihak luar, tinjau aktivitas mereka yang dapat membaca, menghapus, dan mengubah data. Kenali pemakai melalui hal-hal yang mereka ketahui (*password*, PIN, jawaban atas pertanyaan pribadi), atau yang mereka miliki (kartu identitas, kartu pegawai aktif), atau melalui karakteristik

Tabel 8-3
Ringkasan Pengendalian Pengamanan Utama (*lanjutan*)

Kategori Pengendalian	Ancaman/Risiko	Pengendalian
		personal mereka (sidik jari, pola suara, pemindai retina, bentuk wajah, tanda tangan, dan sistem sandi tekan), pemeriksaan kesesuaian, matriks pengendalian akses.
Perlindungan atas PC dan jaringan klien/server	Kerusakan file komputer dan perlengkapannya; akses yang tidak memiliki otorisasi ke data rahasia; pemakai yang tidak dikenali sistem pengamanan	Lakukan inventori atas PC dan pemakainya, sesuaikan sistem pengamanan dengan ancaman dan risikonya, latih pemakai tentang pengendalian PC, kunci *disk drive*, beri label yang tidak dapat dilepas, batasi data yang disimpan atau yang di-*download*, larang software personal atau mengkopi software perusahaan untuk penggunaan personal, simpan data yang sensitif dalam tempat yang aman, secara otomatis mematikan jaringan PC yang tidak digunakan, buat cadangan *hard drive* secara teratur, enkripsi file atau beri file *password*, hapus bersih disk dengan menggunakan *program utility*, buat dinding pelindung di sekitar sistem operasi, *boot* PC dalam sistem pengamanan, gunakan pengendalian *password* bertingkat, pekerjakan spesialis atau program pengamanan untuk mendeteksi kelemahan di jaringan, audit dan catat pelanggaran pengamanan.
Pengendalian Internet dan *e-commerce*	Kerusakan file data dan perlengkapan; akses yang tidak memiliki otorisasi ke data rahasia	*Password*, enkripsi, verifikasi *routing*, software pendeteksi virus, *firewall*, pembuatan jalur khusus, penggunaan amplop elektronis, tolak akses pegawai ke Internet, dan server Internet tidak terhubung dengan komputer lainnya di perusahaan.

Keterpeliharaan

- 2 Kategori Keterpeliharaan
  - Pengembangan proyek dan pengendalian akuisisi
  - Perubahan Pengendalian manajemen

Pengembangan proyek dan pengendalian akuisisi

- Termasuk:
  - Rencana Utama Strategis
  - Pengendalian Proyek
  - Jadwal Pemrosesan Data
  - Pengukuran Kinerja sistem
  - Peninjauan Pascaimplementasi

Perubahan Pengendalian Manajemen

- Termasuk :
  - Peninjauan secara berkala terhadap semua sistem untuk mengetahui perubahan yang dibutuhkan.
  - Semua permintaan diserahkan kepada format yang baku.
  - Pencatatan dan peninjauan permintaan perubahan dan penambahan sistem dari pemakai yang diotorisasi.
  - Penilaian dampak perubahan yang diinginkan terhadap tujuan, kebijakan dan standar keandalan sistem. dll.

Tabel 8-4
Ringkasan Pengendalian Keterpeliharaan Utama

Kategori Pengendalian	Ancaman/Risiko	Pengendalian
Pengembangan proyek dan pengendalian akuisisi	Proyek pengembangan sistem mengkonsumsi sumber daya yang sangat banyak	Rencana utama strategis jangka panjang, jadwal pemrosesan data, penugasan setiap proyek ke manajer atau tim, rencana pengembangan proyek, kejadian penting dari proyek, evaluasi kinerja, pengukuran kinerja sistem (pemasukan data, penggunaan, waktu respons), dan peninjauan pascaimplementasi.
Perubahan pengendalian manajemen	Proyek pengembangan sistem mengonsumsi sumber daya yang sangat banyak, perubahan sistem yang tidak diotorisasi	Perubahan kebijakan dan prosedur pengendalian manajemen, peninjauan berkala semua sistem untuk kebutuhan perubahan, format baku untuk perubahan, pencatatan dan peninjauan permintaan perubahan, penilaian dampak perubahan terhadap keandalan sistem, pengkategorian dan penyusunan semua perubahan, prosedur untuk mengatasi hal-hal yang mendadak, pengkomunikasian perubahan ke manajemen dan pemakai, persetujuan manajemen terhadap perubahan, penugasan tanggung jawab khusus ketika mempertahankan sejumlah tugas, pengontrolan hak akses sistem, pemastian bahwa perubahan melewati semua langkah yang sesuai, pengujian semua perubahan, pengembangan rencana untuk melindungi perubahan sistem yang kritis, implementasi fungsi kepastian kualitas, dan pembaruan dokumentasi dan prosedur.

Integritas

- Sebuah Organisasi mendesain pengendalian umum untuk memastikan bahwa lingkungan pengendalian berdasarkan komputer dari organisasi yang stabil dan dikelola dengan baik.
- Pengendalian Aplikasi digunakan untuk melindungi, mendeteksi dan mengkoreksi kesalahan dalam transaksi ketika mengalir melalui berbagai tahap program pemrosesan data.

Integritas : Pengendalian Sumber Data

Termasuk :

- Desain Formulir
- Pengujian Urutan Formulir
- Dokumen Berputar
- Pembatalan dan penyimpanan dokumen
- Otorisasi dan kumpulan tugas
- Visual scanning
- Verifikasi digit pemeriksaan
- Verifikasi Kunci

Itegritas:
Rutinitas Validasi Input

Termasuk :

- Sequence check
- Field check
- Sign check
- Validity check
- Capacity check
- Limit check
- Range check
- Reasonableness test
- Redundant data check

Integrity:
Pengendalian Entry Data On-Line

Sasaran dari pengendalian entri data on-line adalah untuk memastikan integritas data transaksi yang dimasukan dari terminal on-line dan PC dengan mengurangi kesalahan dan penghilangan.

Termasuk :

- Field, limit, range, reasonableness, sign, validity, redundant data checks
- User ID numbers
- Compatibility tests
- Automatic entry of transaction data, where possible
- Prompting
- Preformatting
- Completeness check
- Closed-lop verification
- Transaction log
- Error messages

Integritas : Pengendalian pemrosesan dan penyimpanan data

Termasuk :

- Kebijakan dan Prosedur
- Fungsi pengendalian Data
- Prosedur Rekonsiliasi
- Rekonsiliasi data eksternal
- Pelaporan penyimpangan
- Pemeriksaan sirkulasi data
- Pencocokan data
- Label file
- Mekanisme perlindungan penulisan
- Mekanisme perlindungan database
- Pengendalian Konversi data
- Pengamanan data

Pengendalian Output

- Ancaman/Resiko
  - Output komputer yang tidak akurat dan tidak lengkap.
- Pengendalian
  - Prosedur untuk memastikan bahwa output sistem sesuai dengan tujuan integritas, kebijakan dan standar organisasi
  - Peninjauan visual output komputer
  - Rekonsiliasi jumlah total batch
  - Distribusi output secara tepat
  - Otuput rahasia yang dikirim telah dilindungi dari akses dan modifikasi dari yang tdk memiliki otorisasi, serta kesalahan pengiriman. dll

Pengendalian Transmisi Data

- Ancaman/Resiko
  - Akses yang tidak memiliki otorisasi terhadap data yang ditransmisi atau kesistem itu sendiri, kegagalan sistem dan kesalahan sistem dalam transmisi data.
- Pengendalian
  - Awasi jaringan untuk mendeteksi poin-poin yang lemah
  - Backup komponen
  - Desain jaringan untuk mengatasi pemrosesan puncak
  - Multijalur komunikasi antara komponen jaringan
  - Pemeliharan pencegahan
  - Ekripsi data
  - Verifikasi Routing
  - Pemeriksaan kesamaan dan prosedur pengenalan pesan.

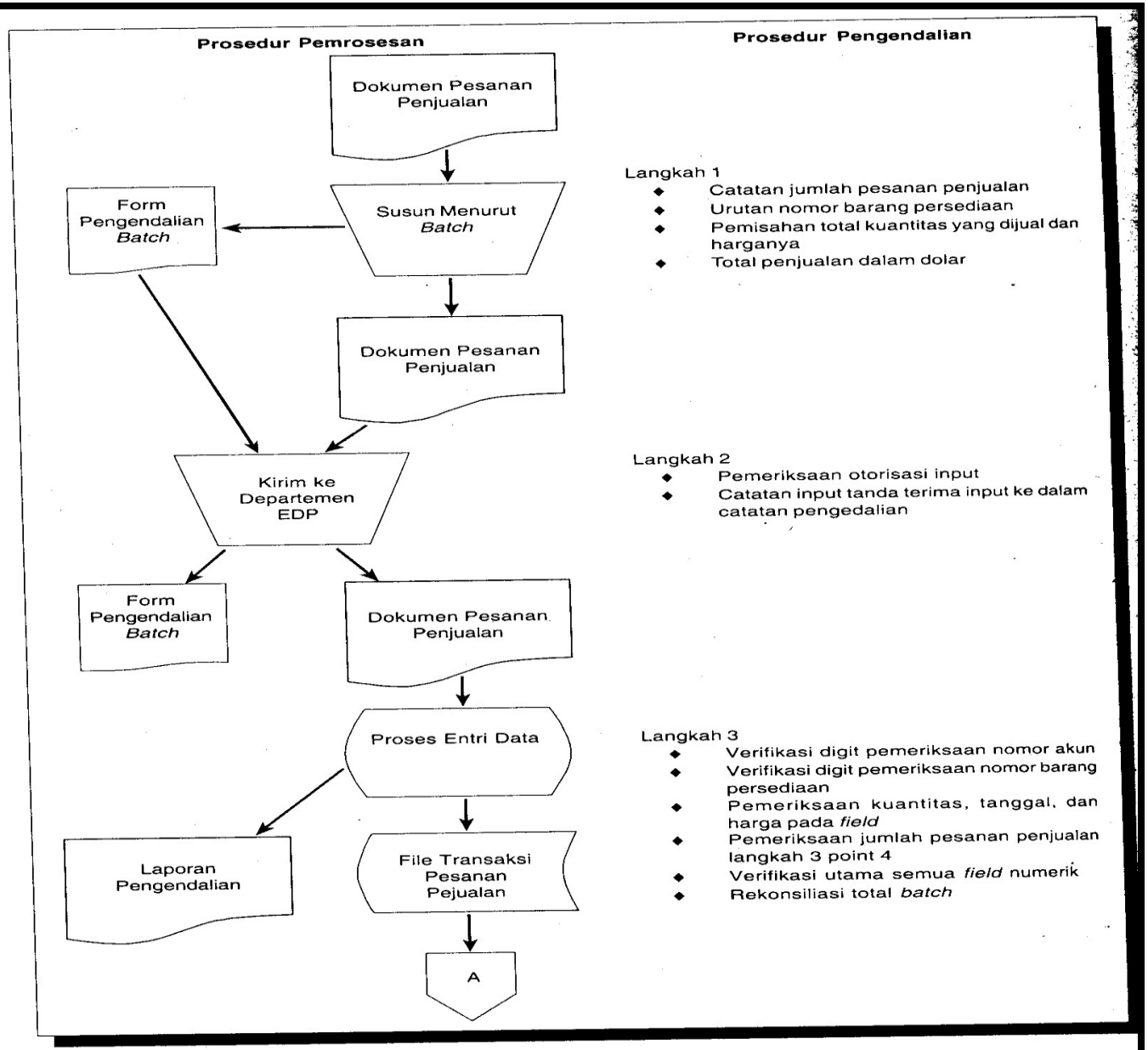
Tabel 8-5
Ringkasan Pengendalian Integritas Utama

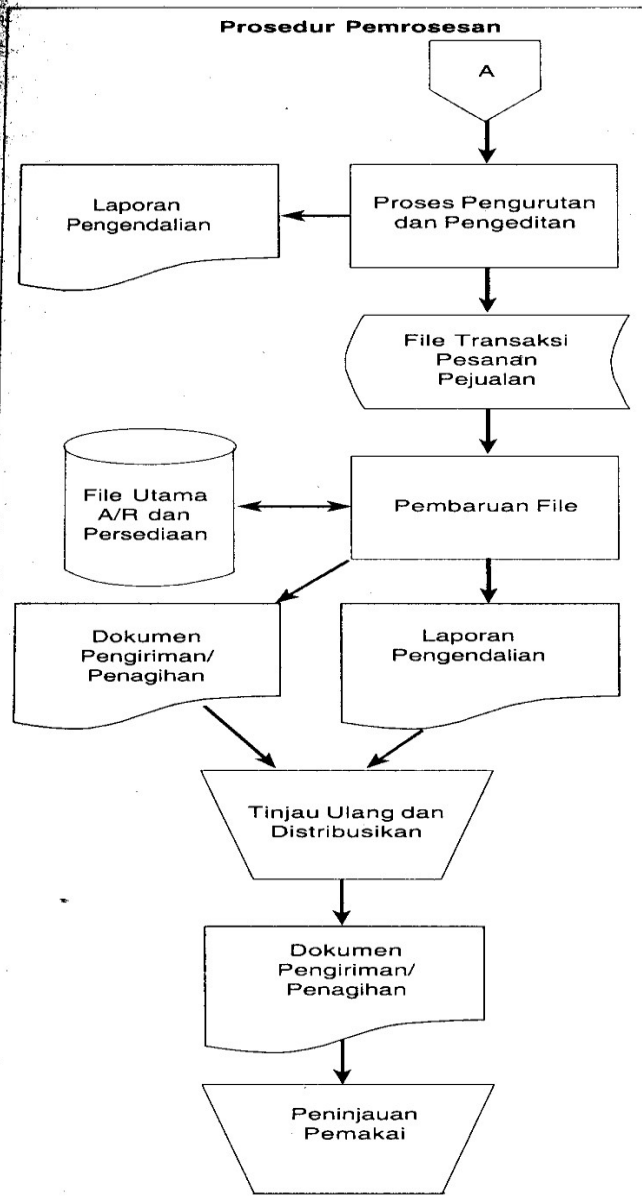
Kategori Pengendalian	Ancaman/Risiko	Pengendalian
Pengendalian sumber data	Input data yang tidak valid, tidak lengkap, atau tidak akurat	Desain formulir, formulir yang diberi nomor secara berurutan, dokumen berputar, pembatalan dan penyimpanan dokumen, peninjauan otorisasi yang sesuai, kumpulan tugas, pemindai visual, verifikasi digit pemeriksaan, dan verifikasi kunci.
Rutinitas validasi input	Data yang tidak valid atau tidak akurat dalam file transaksi yang diproses oleh komputer	Pada saat file transaksi diproses, program edit memeriksa *field* data utama yang menggunakan pemeriksaan edit tersebut: urutan, *filed*, tanda, validitas, batas, jangkauan, kelogisan, data yang berlebihan, dan pemeriksaan kapasitas. Masukan pengecualian ke dalam catatan kesalahan; selidiki, koreksi, dan masukan kembali secara tepat waktu; edit kembali; dan siapkan ringkasan laporan kesalahan.
Pengendalian entri data *on-line*	Input transaksi yang tidak valid atau tidak akurat yang dimasukkan melalui terminal *on-line*	Pemeriksaan *field*, batasan, jangkauan, kelogisan, tanda, validitas, dan data yang redundan; ID pemakai dan *password*; pengujian kompatibilitas; sistem entri data secara otomatis; pemberitahuan ke operator selama entri data; prapemformatan; pengujian kelengkapan; verifikasi *closed-loop*; catatan transaksi yang dipertahankan oleh sistem; pesan kesalahan yang jelas; dan penyimpanan data yang cukup untuk memenuhi persyaratan legal.
Pengendalian pemrosesan dan penyimpanan data	Data yang tidak akurat atau tidak lengkap dalam file utama yang diproses oleh komputer	Kebijakan dan prosedur (menentukan aktivitas pemrosesan data dan personil bagian penyimpanannya; pengamanan dan kerahasiaan data; jejak audit; serta kesepakatan kerahasiaan); mengawasi dan mempercepat entri data oleh personil pengendalian data; rekonsiliasi pembaruan sistem dengan akun pengendali atau laporan; rekonsiliasi jumlah total dalam database dengan jumlah total yang dibuat secara

Tabel 8-5
Ringkasan Pengendalian Integritas Utama (*lanjutan*)

Kategori Pengendalian	Ancaman/Risiko	Pengendalian
		terpisah; pelaporan penyimpangan, pemeriksaan sirkulasi data, nilai *default*; pencocokkan data; pengamanan data (perpustakaan data dan pustakawan, kopi cadangan file data yang disimpan di lokasi luar yang aman, perlindungan dari kondisi yang dapat merusak data yang disimpan); penggunaan label nama file serta mekanisme perlindungan penulisan; mekanisme perlindungan database (administrator database, kamus data, dan pengendalian pembaruan simultan); serta pengendalian konversi data.
Pengendalian output	Output komputer yang tidak akurat dan tidak lengkap	Prosedur untuk memastikan bahwa output sistem sesuai dengan tujuan integritas, kebijakan, dan standar organisasi; peninjauan visual output komputer; rekonsiliasi jumlah total *batch*; distribusi output secara tepat; output rahasia yang dikirim telah dilindungi dari akses dan modifikasi yang tidak memiliki otorisasi, serta kesalahan pengiriman; output rahasia atau bersifat sensitif disimpan dalam area yang aman; pemakai meninjau kelengkapan dan akurasi output komputer; menyobek output rahasia yang tidak lagi dibutuhkan; laporan kesalahan dan penyimpangan.
Pengendalian transmisi data	Akses yang tidak memiliki otorisasi terhadap data yang ditransmisi atau ke sistem itu sendiri; kegagalan sistem; kesalahan dalam transmisi data	Awasi jaringan untuk mendeteksi poin-poin yang lemah, *back-up* komponen, desain jaringan untuk mengatasi pemrosesan puncak, multijalur komunikasi antara komponen jaringan, pemeliharaan pencegahan, enkripsi data, verifikasi *routing* (label judul, skema pembuktian keaslian bersama, sistem pemanggilan kembali), pemeriksaan kesamaan, dan prosedur pengenalan pesan (pemeriksaan bergema, label percobaan, *batch* bernomor).

Gambar 8-4
Bagan Alir Pemrosesan Pesanan Penjualan dan Prosedur Pengendalian yang Berkaitan





Prosedur Pengendalian

Langkah 4
- Pemeriksaan urutan nomor akun
- Pemeriksaan batas kuantitas dan harga
- Pemeriksaan jangkauan tanggal pengiriman
- Pengujian kelengkapan keseluruhan catatan
- Rekonsiliasi total *batch*
- Peninjauan kesalahan yang teridentifikasi dengan pemeriksaan edit
- Penelitian dan koreksi input yang salah

Langkah 5
- Pengamanan file utama dalam perpustakaan file
- Perlindungan file utama dengan menggunakan label file
- Pemeliharaan salinan file utama
- Pemeriksaan validitas nomor akun pelanggan
- Pemeriksaan validitas nomor barang persediaan
- Pemeriksaan tanda kuantitas persediaan yang ada sekarang
- Pemeriksaan batas jumlah penjualan dengan batas kredit
- Pemeriksaan jangkauan harga penjualan
- Pengujian kelogisan jumlah yang dipesan
- Pemeriksaan data redundan pada data pelanggan
- Pemeriksaan data redundan pada data persediaan

Langkah 6
- Rekonsiliasi total *batch*
- Peninjauan kesalahan yang diidentifikasi oleh pemeriksaan edit
- Investigasi dan koreksi input yang salah
- Distribusi dokumen penagihan dan pengiriman
- Pencatatan distribusi output pada catatan pengendalian
- Pengembalian file utama ke perpustakaan file

Langkah 7
- Inspeksi visual terhadap output
- Rekonsiliasi total *batch*

Gambar 8-4
Bagan Alir Pemrosesan Pesanan Penjualan dan Prosedur Pengendalian yang Berkaitan (*lanjutan*)