MSIM4305
Edisi 1

MODUL 01

Audit Sistem Informasi

Inayatulloh, SE., MMSI.

Daftar Isi

Pendahuluan

Audit sistem informasi merupakan bagian penting setelah membangun sistem informasi. Sebagai mahasiswa sistem informasi Anda sudah memahami dengan baik proses pembangunan sebuah aplikasi atau sistem informasi dengan metode *waterfall* dan SDLC (*System Development Life Cycle*), dimana metode tersebut ditutup pada proses implementasi. Namun metode tersebut tidak secara detail membahas bagaimana mekanisme dari evaluasi sistem yang sudah dibangun. Disinilah peran dari audit sistem informasi dimana proses penilaian yang dilakukan lebih dalam dengan melihat efektivitas penggunaan teknologi informasi untuk mendukung tujuan perusahaan. Oleh karena itu, yang pertama kali dibahas adalah pengertian dari audit sistem informasi dan pengendalian sistem informasi. Dengan memahami pengendalian sistem informasi akan memudahkan kita melakukan audit sistem informasi karena sistem yang terkendali akan memudahkan penelusuran semua proses yang berhubungan dengan sistem informasi.

Setelah mempelajari modul ini Anda diharapkan akan dapat memahami tentang audit sistem informasi. Secara lebih rinci Anda diharapkan mampu menjelaskan definisi pengendalian dan keamanan sistem informasi dengan rincian memahami:

1. audit sistem informasi,
2. pengendalian atau kontrol dalam sistem informasi,
3. jenis pengendalian sistem informasi,
4. keamanan sistem informasi terkait dengan proses audit sistem informasi,
5. konsep komunikasi terkait dengan audit sistem informasi.

Kegiatan Belajar 1

Kontrol dalam Sistem Informasi

Audit sistem informasi adalah proses pengumpulan dan penilaian bukti-bukti untuk menentukan apakah sistem komputer dapat mengamankan aset, memelihara integritas data, dapat mendorong pencapaian tujuan organisasi secara efektif dan menggunakan sumberdaya secara efisien dan pengendalian dari sistem informasi merupakan bagian penting dari audit sistem informasi karenanya diperlukan pemahaman yang lebih dalam tentang bagaimana perbandingan sistem manual dengan sistem informasi. Beberapa perubahan mendasar dari sistem manual ke sistem berbasis komputer sebagai berikut.

1. Sistem informasi sering kali jauh lebih kompleks daripada sistem manual, sebagai contoh sistem berbasis komputer setidaknya membutuhkan sejumlah teknisi komputer yang sangat terampil untuk mengembangkan dan memeliharanya dibandingkan dengan sistem manual, namun hasil dari sistem komputer pasti jauh lebih baik dibandingkan sistem manual.
2. Sistem informasi memiliki kemampuan memproses data dalam jumlah besar dengan kecepatan tinggi, dan dapat mengirimkan data efektif secara instan pada jarak yang ekstrim tanpa batas ruang dan waktu.
3. Sistem informasi menyimpan data dalam bentuk elektronik sehingga dibutuhkan alat khusus dan kemampuan khusus yang seringkali lebih kompleks untuk auditor dibandingkan memeriksa catatan kertas. Selain itu, sistem informasi seringkali mengabaikan cetak kertas karena hampir seluruh aktivitas dan rekam jejaknya disimpan di media elektronik.
4. Sistem informasi memproses data secara otomatis dengan sedikit sekali intervensi manual di dalamnya.
5. Saat ini sistem berbasis informasi hampir seluruh proses dilakukan secara otomatis. Paradigma lama keberadaan teknologi bertujuan untuk mengurangi penggunaan tenaga kerja karena beberapa kelebihan yang dimiliki sistem berbasis komputer. Tapi saat ini paradigma tersebut bergeser dimana tujuannya bukan mengurangi tenaga kerja tapi lebih kepada peningkatan efektifitas dan efsiensi proses bisnis sehingga harus menggunakan sistem berbasis komputer. Keharusan menggunakan sistem berbasis komputer yang berdampak pada efektifitas dan efisiensi proses bisnis karena para pesaing melakukan hal yang sama untuk dapat menguasai pasar. Kemampuan teknologi informasi tidak saja

hanya membantu tugas-tugas pada tingkat operasional tapi kemampuan teknologi informasi juga dapat digunakan untuk level manajemen strategi. Sebagai contoh kemampuan kecerdasan buatan menjadikan tugas dan tanggung jawab seorang dengan level manajemen strategi dapat dilakukan dengan cepat dan keakuratan yang tinggi. Dengan demikian fungsi pengawasan dan pemeriksaan relatif lebih mudah karena semua data, proses dan semua aktivitas terekam dalam sistem.

6. Proses bisnis perusahaan yang menggunakan teknologi informasi secara konsisten dapat diawasi dengan tingkat keakuratan yang tinggi dan tingkat pengendalian yang tinggi karena saat ini hampir semua perusahaan menggunakan sistem yang terintegrasi antar semua bagian baik pihak internal maupun ekstenal dan semuanya terekam dalam data digital.
7. Dalam sistem informasi yang besar, terdapat konsentrasi risiko yang signifikan karena aset sumber daya informasi organisasi dalam satu tempat namun hal ini bisa dikurangi dengan membuat beberapa media penyimpanan yang berbeda lokasi dan dapat digunakan jika tempat penyimpanan utama mengalami masalah.
8. Penggunaan teknologi informasi yang sangat mendasar pada hampir semua proses bisnis perusahaan tentu akan merubah batasan hukum yang berbeda dari sistem manual. Dalam kontes audit atau pemeriksaan sistem informasi maka batasan hukum menjadi hal yang sangat penting.
9. *Requirement* terhadap tenaga ahli yang memiliki kemampuan menganalisis data berbasis komputer dan memahami batasan hukum umumnya sekarang menjadi salah satu cara praktis untuk menganalisis data perusahaan.
10. Selain itu, penggunaan sistem informasi dengan prosedur terprogram memungkinkan proses audit mengadopsi pendekatan sistem di mana kontrol dalam proses sistem komputer lebih konsisten daripada sistem manual. Dalam sistem manual kualitas prosedur kontrol dapat berubah, tergantung pada kualitas staf dan konsistensi kerja mereka. Hal ini dapat mengakibatkan proses audit harus dilakukan dengan sejumlah besar pemeriksaan transaksi, untuk mengkonfirmasi transaksi telah diproses dengan benar.

A. JENIS PENGENDALIAN DALAM SISTEM INFORMASI DALAM AUDIT SI

Pengendalian pada sistem informasi secara umum diklasifikasikan menjadi dua bagian besar.

1. Pengendalian Umum

   Adalah pengendalian yang mengatur lingkungan di mana sistem informasi dibangun, dikembangkan, dipelihara, dan dioperasikan. Pengendalian yang mencakup standar pembangunan dan pengembangan sistem yang dioperasikan oleh organisasi, pengendalian yang berlaku untuk pengoperasian instalasi

komputer termasuk didalamnya perangkat keras, perangkat lunak, teknologi jaringan dan semua bagian yang berhubungan dengan sistem berbasis komputer.

2. Pengendalian aplikasi atau sistem informasi, baik manual dan terkomputerisasi, dalam aplikasi bisnis untuk memastikan data tersebut diproses secara lengkap, akurat, dan tepat waktu. Kontrol aplikasi biasanya khusus untuk aplikasi bisnis dan termasuk:
   a. Kontrol *input* seperti validasi dan *batching data*. Proses sebuah sistem dimulai pada aktivitas *input* data untuk kemudian diolah oleh sistem. *Input* data perlu serangkaian proses validasi yang harus dilaksanakan untuk dapat menggunakan sistem seperti memasukkan *user id* dan *password* jika menggunakan layar komputer atau *keyboard* sebagai media *input*nya. Proses yang berbeda jika sistem menggunakan alat yang berbeda sebagai media *input* sebagai contoh *finger scanner* atau RFID *(Radio Frequnce Identification)* atau *QRcode*. Kesimpulannya pengendalian sistem informasi bergantung pada *device* yang digunakan. Yang kedua terkait dengan *batching data* yang tersimpan dalam sistem harus melalui serangkaian proses validasi untuk memastikan bahwa data yang akan disimpan sudah mengikuti ketentuan yang ada.
   b. Pengendalian *run-to-run* untuk memeriksa total *file* pada masukan *(input)*, proses *(process)* dan keluaran *(output)* dari sistem yang digunakan. Pengendalian pada bagian ini sangat penting untuk memastikan secara kuantitas *file* yang digunakan tidak mengalami pengurangan saat proses dilakukan. Pengurangan yang dimaksud adalah informasi yang dihasilkan tidak valid karena mengalami kesalahan saat pemrosesan berlangsung, misalnya salah perhitungan yang disebabkan kesalahan pemrograman komputer.

Pada akhirnya proses audit adalah menentukan apakah sistem aplikasi berfungsi sebagaimana mestinya, integritas, akurasi, dan kelengkapan data terkontrol dengan baik, dan melaporkan setiap perbedaan yang signifikan. Integritas data bergantung pada kecukupan kontrol aplikasi. Namun, kontrol aplikasi sepenuhnya bergantung pada integritas kendali umum atas lingkungan di dalamnya yang mana aplikasi dikembangkan dan dijalankan.

Proses audit sering mengambil posisi yang cukup ketergantungan pada kontrol di sekitar komputer, yaitu dalam kontrol aplikasi atau sistem informasi karena auditor berkonsentrasi pada *input* dan *output* dari komputer, bukan apa yang terjadi pada komputer.

Dengan penyebaran kerja *online* dan *real time*, dan dari meningkatnya kapasitas penyimpanan yang fleksibel, semua data organisasi biasanya dimuat secara permanen di sistem komputer dan dapat diakses dari berbagai tempat, dengan hanya melakukan kontrol terhadap perangkat lunak sistem yang mengendalikan akses ke data. Sistem ini

secara teknis meningkatkan kompleksitas namun potensi untuk memanfaatkan kelemahan yang ada juga meningkat.

Sangatlah penting bahwa pemeriksaan yang akan dilakukan mengintegrasikan semua bagian yang ada pada sistem yang digunakan perusahaan. Auditor harus memiliki pengetahuan dalam fasilitas yang disediakan dalam perangkat lunak sistem utama dalam organisasi yang sedang diaudit. Jenis pengendalian keamanan sistem informasi berdasarkan bentuknya terbagi atas kontrol keamanan fisik dan kontrol keamanan logis.

1. Kontrol Keamanan Fisik

Kontrol keamanan fisik meliputi semua perangkat keras komputer termasuk CPU dan semua perangkat periferal. Dalam sistem jaringan, perangkat ini mencakup semua *bridge*, *router*, *gateway*, sakelar, modem, hub, media telekomunikasi, dan perangkat lain yang digunakan dalam transmisi fisik data. Peralatan ini harus dilindungi secara memadai dari kerusakan fisik akibat bencana alam, seperti gempa bumi, angin topan, tornado, dan banjir, serta bahaya lainnya, seperti pemboman, kebakaran, lonjakan listrik, pencurian, vandalisme, dan gangguan lainnya. Kontrol yang melindungi dari ancaman ini disebut kontrol keamanan fisik. Contoh kontrol keamanan fisik mencakup berbagai jenis perlindungan (misalnya, kunci konvensional, akses elektronik, biometrik, *password*); perlindungan asuransi atas perangkat keras dan biaya untuk membuat ulang data; prosedur untuk melakukan pencadangan harian perangkat lunak sistem, program aplikasi, dan data; serta penyimpanan atau *backup*.

Dalam proses audit sistem informasi terkait dengan *hardware* harus meliputi beberapa proses untuk memastikan semua proses dari mulai pengadaan perangkat keras dari *supplier* hingga pembuangan perangkat keras ketika sudah habis umur ekonomisnya memenuhi standard keamanan perusahaan. Berikut ini adalah tahapan-tahapan yang harus dilakukan untuk melindungi keamanan data yang berhubungan dengan perangkat keras.

a. Perencanaan, yaitu kegiatan membuat rencana semua kegiatan yang dilakukan selama kegiatan audit sistem informasi.
b. *Acquisistion* adalah kegiatan menganalisis sumber perangkat keras yang digunakan oleh perusahaan untuk mendukung sistem informasi yang digunakan oleh perusahaan.
c. *Implementation* adalah kegiatan memahami dan mengawasi instalasi perangkat keras yang digunakan untuk mendukung sistem informasi perusahaan.
d. *Maintenance* adalah kegiatan memahami proses pemeliharaan perangkat keras yang digunakan untuk mendukung sistem informasi perusahaan.
e. Disposal adalah kegiatan mengetahui kegiatan pembuangan perangkat keras pendukung sistem informasi perusahaan yang sudah tidak digunakan lagi.

Proses audit sistem informasi yang berhubungan dengan perangkat keras fokus pada 4 hal.

a. Efektivitas dan efisiensi penggunaan aset perangkat keras. Efektivitas dan efisiensi pada biaya dan manfaat dari perangkat keras yang digunakan artinya biaya atau harga dari perangkat keras yang dibeli harus berdasarkan manfaat yang dihasilkan sehingga tercipta efektivitas dan efisiensi yang tinggi.
b. Sistem keamanan sebagai perlindungan aset perangkat keras. Sistem pengamanan aset perangkat keras meliputi lokasi atau gedung tempat penyimpanan dan semua sub sistem di dalamnya seperti tenaga keamanan, pendukung jika terjadi bencana alam termasuk *backup* data pada lokasi yang berbeda.
c. Ketersediaan penggunaan perangkat keras bagi pihak yang berwenang merupakan salah satu hal penting sehingga penggunaan perangkat keras dapat ditelusuri penggunaannya, jika terdapat kerusakan atau penyalahgunaan dapat dengan mudah ditindak lanjuti.
d. Pemeliharaan aset perangkat keras secara terintegrasi menekankan pada kondisi dimana penggunaan aset perangkat keras tidak berdiri sendiri artinya penggunaan perangkat keras berhubungan satu dengan lainya. Oleh karena itu pemeliharaan perangkat keras harus dilakukan secara terpadu.

2. Kontrol Keamanan Logis

Kontrol keamanan logis adalah perlindungan keamanan atas sistem komputasi secara memadai dari akses yang tidak sah dan kerusakan yang tidak disengaja atau disengaja atau perubahan program perangkat lunak sistem, program aplikasi, dan data. Perlindungan dari ancaman ini dilakukan melalui penerapan kontrol keamanan logis. Kontrol keamanan logis adalah kontrol yang membatasi kapabilitas akses pengguna sistem dan mencegah pengguna yang tidak berwenang mengakses sistem. Kontrol keamanan logis ada di dalam sistem operasi, sistem manajemen *database*, program aplikasi, atau ketiganya.

Jumlah dan jenis kontrol keamanan logis yang tersedia bervariasi dengan setiap sistem operasi, sistem manajemen basis data, aplikasi, dan banyak jenis perangkat telekomunikasi. Beberapa dirancang dengan berbagai pilihan kontrol keamanan logis dan parameter yang tersedia untuk administrator keamanan sistem. Ini termasuk ID pengguna, kata sandi dengan persyaratan panjang minimum dan jumlah digit dan karakter yang diperlukan, penangguhan ID pengguna setelah upaya masuk yang gagal berturut-turut, pembatasan akses direktori dan *file*, pembatasan waktu dan hari, dan pembatasan penggunaan terminal. Sistem operasi dan aplikasi lain dirancang dengan sedikit pilihan kontrol. Untuk sistem ini, kontrol keamanan logis sering ditambahkan sebagai alternatif saja, mengakibatkan pengaturan kontrol yang lebih lemah daripada yang diinginkan, bahkan ketika pembatasan akses maksimum yang tersedia telah diterapkan.

Banyak sistem diprogram dengan kontrol yang sepadan dengan tingkat risiko yang terkait dengan fungsi yang dilakukan oleh sistem. Namun, waspadalah terhadap sistem berisiko tinggi dengan kontrol yang buruk. Banyak sistem berisiko tinggi telah diprogram dengan fitur kontrol yang tidak memadai atau memiliki fitur kontrol yang memadai, tetapi fitur tersebut tidak diimplementasikan secara memadai. Masalah dapat terjadi ketika pemrogram dan/ atau pemilik proses tidak menyadari satu atau lebih risiko signifikan yang dihadapi organisasi selama penggunaan sistem.

B. KEAMANAN SISTEM INFORMASI

Keamanan merupakan hal krusial dari sistem *online*. Faktor eksternal merupakan faktor terbesar perusakan yang dilakukan oleh pihak luar seperti *virus, worm, trojan horse* dan lain-lain. Sistem *online* menghubungkan sistem perusahaan ke jaringan seluruh dunia sehingga potensi untuk terkena serangan virus dan lain-lain semakin tinggi sehingga diperlukan sistem keamanan yang lebih memadai untuk melindungi aset informasi perusahaan. Akses tidak sah merupakan ancaman serius dari sistem *online* karena sistem ini terhubung ke seluruh dunia sehingga siapapun dapat mengakses informasi perusahaan jika sistem keamanan sistem *online* tidak diperbaharui secara berkala. Pihak diluar sistem menggunakan berbagai cara dengan memanfaatkan kemajuan teknologi komputer untuk meretas sistem *online* perusahaan maka sistem keamanan yang mendukung sistem *online* perusahaan harus dirancang berlapis untuk meningkatkan keamanan dari akses yang tidak sah.

Perubahan yang tidak disengaja atau disengaja merupakan kesalahan yang disebabkan oleh pihak internal dan eksternal. Perubahan yang tidak disengaja disebabkan kesalahan *user* dalam menggunakan sistem perusahaan sehingga berdampak pada hasil dari pengolahan data yang tidak akurat, tidak valid, dan lain sebagainya. Seharusnya peristiwa ini bisa diminimalisir dengan membuat sebuah perancangan sistem yang lebih menekankan pada antisipasi kemungkinan kesalahan yang dilakukan oleh *user*. Sebagai contoh untuk meningkatkan keamanan *password* maka dirancang sebuah aturan bahwa *password* harus minimal 8 karakter dengan kombinasi huruf, angka dan simbol. Ketika *user* memasukkan *password* yang mudah ditebak dan terlalu sederhana maka sistem akan mengingatkan tentang aturan pembuatan *password* tersebut.

Beberapa bidang yang rentan terhadap ancaman keamanan adalah fitur dari sistem. Dari beberapa kasus yang pernah terjadi adalah *user* tidak dapat mengakses fitur karena fitur sistem tidak dapat di akses. Ada sebuah cara untuk menghambat kinerja sistem atau membuat sistem tidak berjalan yang disebut sebagai *Denial Service of Attack*. Serangan ini menyebabkan sistem tidak dapat diakses karena terlalu banyak pihak yang masuk ke dalam sistem. Dimana pihak yang masuk ke sistem merupakan transaksi semu atau palsu dan tidak memiliki kewenangan untuk masuk ke dalam sistem, sehingga ketika ada *user* dengan transaksi yang sebenarnya ingin masuk, mereka tidak dapat masuk ke sistem tersebut.

Perlindungan harus dilakukan terhadap perangkat keras, perangkat lunak, dan sumberdaya manusia. Perangkat keras dilindungi dari pencurian, sabotase, dan penetrasi. Beberapa sistem keamanan yang dapat diterapkan untuk melindungi aset informasi perangkat keras komputer. Sumberdaya manusia memiliki peran penting dalam menjaga keamanan sistem informasi. Manusia menjadi bagian paling penting karena yang akan menggunakan, mengoperasikan, memprogram, dan mengelola komputer. Terdapat beberapa posisi yang berhubungan dengan sistem informasi.

1. *Programmer* adalah spesialis teknis yang sangat terlatih yang membangun perangkat lunak dengan instruksi untuk komputer. Seorang *programmer* komputer, kadang-kadang disebut sebagai pengembang perangkat lunak atau baru-baru ini juga disebut sebagai pembuat kode (terutama dalam konteks yang lebih informal), adalah orang yang menciptakan perangkat lunak komputer. Istilah *programmer* komputer dapat merujuk pada seorang spesialis dalam satu bidang komputer, atau seorang generalis yang menulis kode untuk berbagai jenis perangkat lunak. Bahasa komputer *programmer* yang paling sering digunakan (mis., Assembly, COBOL, C, C ++, C #, JavaScript, Lisp,) dapat diawali dengan istilah *programmer*. Beberapa orang yang bekerja dengan bahasa pemrograman *web* juga mengawali judul mereka dengan pengembang aplikasi perangkat lunak. Pendidikan yang dibutuhkan adalah gelar Sarjana. Saat ini *programmer* bertanggung jawab untuk membuat dan meningkatkan aplikasi untuk ponsel, tablet, dan perangkat seluler lainnya. Ini adalah karir pemrograman yang ideal untuk seseorang yang memiliki mentalitas "gambaran besar" dan suka berkolaborasi dengan orang lain untuk mewujudkan ide. *Programmer* juga mengetahui dasar-dasar pengkodean dan memiliki bakat untuk matematika.
2. *Web Developer*, dimana tampilan dan fungsi situs *web* adalah hasil langsung dari pekerjaan *web developer* atau pengembang *web*. Semua karier pemrograman membutuhkan kesabaran, tetapi yang ini memberikan kepuasan instan lebih dari kebanyakan. Pengembang *web* mendengarkan dengan baik kebutuhan klien mereka dan pemecahan masalah untuk memberi mereka situs *web* terbaik untuk bisnis mereka. Pengembang *web* berhasil dengan baik ketika mereka dapat menunjukkan portofolio pekerjaan mereka dan memiliki pemahaman yang mendalam tentang pengkodean. Bahasa pemrograman paling umum untuk pengembang *web* adalah JavaScript, Java, HTML5.
3. *Computer Systems Engineer* bertanggung jawab untuk mengidentifikasi solusi untuk masalah aplikasi yang kompleks, masalah administrasi sistem, atau masalah jaringan. Mereka bekerja sama dengan klien atau pemangku kepentingan internal untuk memahami kebutuhan sistem dan berkolaborasi dengan pengembang untuk menentukan solusi yang tepat. Ini adalah karir pemrograman lain yang ideal untuk profesional yang paham bisnis. Bahasa pemrograman paling umum untuk *Computer systems engineer* adalah Python, Java, dan C ++.

4. *Database Administrator (DBA)* bertugas mengamankan, mengatur, dan memecahkan masalah penyimpanan untuk sejumlah besar informasi untuk perusahaan *online*. Mereka yang suka menganalisis dan memulihkan informasi, serta menyelesaikan masalah dengan cepat, ini bisa menjadi karier *coding* untuk mereka. Bahasa pemrograman yang paling umum untuk *database administrator* adalah Python, Java, Oracle PL / SQL
5. *Software Quality Assurance Engineer* berada di awal perangkat lunak dibangun, mendokumentasikan kecacatan, merancang skenario tes, dan membuat manual untuk perangkat lunak baru. Mereka juga meninjau desain perangkat lunak untuk mengetahui fungsionalitas dan potensi masalah. Bahasa pemrograman paling umum Java, Python, dan JavaScript.
6. *Business Intelligence Analyst* dimana pemrograman adalah bonus, tetapi tidak terlalu dibutuhkan oleh jabatan ini. Posisi ini untuk marketer di belakang layar yang mengumpulkan semua fakta tentang produk perangkat lunak dan tren untuk menentukan perangkat lunak mana yang dapat membantu menyelesaikan inisiatif bisnis. Bahasa pemrograman paling umum untuk jabatan ini adalah Python dan Java.
7. Analis sistem merupakan penghubung utama antara kelompok sistem informasi dan seluruh organisasi. Tugas analis sistem adalah menerjemahkan masalah dan persyaratan bisnis menjadi persyaratan dan sistem informasi.
8. Manajer sistem informasi adalah pemimpin tim *programmer* dan analis, manajer proyek, manajer telekomunikasi, atau spesialis *database*. Mereka juga merupakan manajer operasi komputer dan staf entri data. Juga sebagai eksternal spesialis, seperti vendor dan produsen perangkat keras, perusahaan perangkat lunak, dan konsultan, sering berpartisipasi dalam operasi sehari-hari dan jangka panjang perencanaan sebuah sistem informasi.
9. Di banyak perusahaan, departemen sistem informasi dipimpin oleh seorang *Chief Information Officer* (CIO). CIO adalah manajer senior yang mengawasi penggunaan teknologi informasi di perusahaan. CIO diharapkan memiliki latar belakang bisnis yang kuat serta keahlian sistem informasi dan untuk memainkan peran kepemimpinan dalam mengintegrasikan teknologi ke dalam strategi bisnis perusahaan. Perusahaan besar hari ini juga memiliki posisi untuk *Chief Security Officer* (CSO), *Chief Knowledge Officer* (CKO), dan *Chief Privacy officer* (CPO) yang semuanya bekerja sama dengan CIO.
10. *Chief Security Officer* (CSO) bertanggung jawab atas sistem keamanan informasi untuk perusahaan dan bertanggung jawab untuk menegakkan kebijakan keamanan informasi perusahaan. Terkadang posisi ini disebut *Chief Information Staff Officer* (CISO) dimana keamanan sistem informasi berada terpisah dari keamanan fisik. CSO bertanggung jawab untuk mendidik dan melatih pengguna dan spesialis sistem informasi tentang keamanan, pemeliharaan manajemen sadar akan ancaman keamanan dan kerusakan, dan memelihara alat dan kebijakan yang

dipilih untuk mengimplementasikan keamanan. Sistem informasi keamanan dan kebutuhan untuk melindungi data pribadi yang dimilikinya menjadi sangat penting sehingga perusahaan mengumpulkan data pribadi dalam jumlah besar untuk menetapkan posisi CPO.

11. *Chief Privacy officer* (CPO) adalah bertanggung jawab untuk memastikan bahwa perusahaan mematuhi privasi data sesuai dengan hukum yang berlaku.
12. *Chief knowledge officer* (CKO) bertanggung jawab atas pengetahuan perusahaan program manajemen. CKO membantu merancang program dan sistem untuk menemukan sumber pengetahuan baru atau untuk memanfaatkan pengetahuan yang ada dengan lebih baik dalam proses organisasi dan manajemen.
13. *Network administrator* adalah orang yang ditunjuk dalam sebuah organisasi yang tanggung jawabnya mencakup pemeliharaan infrastruktur komputer dengan penekanan pada jaringan. Tanggung jawab dapat bervariasi antar organisasi, tetapi server di tempat, interaksi jaringan perangkat lunak, serta integritas/ ketahanan jaringan adalah area fokus utama. Peran administrator jaringan dapat sangat bervariasi tergantung pada ukuran, lokasi, dan pertimbangan sosial ekonomi organisasi. Beberapa organisasi bekerja pada rasio dukungan pengguna-ke-teknis, sementara yang lain menerapkan banyak strategi lain. Secara umum, dalam hal situasi reaktif (yaitu: gangguan tak terduga pada layanan, atau peningkatan layanan), Insiden Dukungan TI dimunculkan melalui sistem *problem tracking* . Biasanya, masalah bekerja melalui *helpdesk* dan kemudian mengalir ke area teknologi yang relevan untuk diselesaikan. Dalam kasus masalah terkait jaringan, masalah akan diarahkan ke administrator jaringan. Jika administrator jaringan tidak dapat menyelesaikan masalah, problem akan diteruskan ke teknisi jaringan yang lebih senior untuk pemulihan layanan atau kelompok keterampilan yang lebih sesuai. Administrator jaringan sering terlibat dalam pekerjaan proaktif. Jenis pekerjaan ini sering kali mencakup: pemantauan jaringan, menguji kelemahan jaringan, mengawasi pembaruan yang dibutuhkan, menginstal dan menerapkan program keamanan, dalam banyak kasus, filter *e-mail* dan internet, mengevaluasi jaringan pelaksana. Administrator jaringan bertanggung jawab untuk memastikan bahwa perangkat keras komputer dan infrastruktur jaringan yang terkait dengan jaringan data organisasi dipelihara secara efektif. Di organisasi yang lebih kecil, mereka biasanya terlibat dalam pengadaan perangkat keras baru, peluncuran perangkat lunak baru, memelihara citra disk untuk pemasangan komputer baru, memastikan bahwa lisensi dibayar dan mutakhir untuk perangkat lunak yang membutuhkannya, mempertahankan standar untuk instalasi server dan aplikasi, memantau kinerja jaringan, memeriksa pelanggaran keamanan, dan praktik manajemen data yang buruk. Pertanyaan umum untuk administrator jaringan bisnis kecil-menengah (UKM) adalah, berapa banyak *bandwidth* yang diperlukan untuk menjalankan bisnis? Biasanya, dalam organisasi yang lebih besar, peran ini dibagi menjadi

beberapa peran atau fungsi di berbagai divisi dan tidak dilakukan oleh satu individu. Di organisasi lain, beberapa peran yang disebutkan ini dilakukan oleh administrator sistem. Seperti banyak peran teknis, posisi administrator jaringan memerlukan pengetahuan teknis yang luas dan kemampuan untuk mempelajari seluk beluk jaringan baru dan paket perangkat lunak server dengan cepat. Dalam organisasi yang lebih kecil, peran yang lebih senior dari insinyur jaringan terkadang dilampirkan pada tanggung jawab administrator jaringan. Organisasi yang lebih kecil biasanya melakukan *outsourcing* untuk fungsi ini.

14. *End user* atau pengguna akhir adalah perwakilan dari departemen di luar informasi grup sistem untuk siapa aplikasi dikembangkan. Para pengguna ini sedang memainkan peran yang semakin besar dalam perancangan dan pengembangan sistem informasi. Pada tahun-tahun awal komputasi, kelompok sistem informasi yang dibentuk kebanyakan adalah *programmer* yang memiliki kinerja sangat terspesialisasi tetapi teknis dan terbatas fungsi. Saat ini, semakin banyak jumlah anggota staf yang merupakan analis sistem dan spesialis jaringan, dengan departemen sistem informasi bertindak sebagai agen perubahan yang kuat dalam organisasi. Departemen sistem informasi menyarankan strategi bisnis baru dan produk berbasis informasi baru dan layanan, serta mengkoordinasikan pengembangan teknologi dan perubahan yang direncanakan dalam organisasi.

C. KONSEP KOMUNIKASI AUDIT SISTEM INFORMASI

Penggunaan jenis sarana komunikasi akan mempengaruhi keserempakan waktu komunikasi. Terdapat 2 jenis komunikasi daring yaitu:

1. Komunikasi daring sinkron (serempak) yaitu komunikasi *online* yang dilakukan secara bersamaan dan menggunakan media komputer untuk komunikasi dengan konsep waktu *realtime*. Contoh komunikasi sinkron antara lain sebagai berikut.
   a. *Text chat* adalah sebuah fitur dari jaringan komputer untuk berkomunikasi sesama pengguna komputer yang terhubung pada jaringan internet dimana semuanya sedang dalam jaringan atau *online*. Komunikasi teks dapat mengirim pesan dengan teks kepada orang lain yang sedang daring, kemudian orang yang dituju membalas pesan dengan teks, demikian seterusnya. Itulah proses terjadinya *text chatting*.
   b. *Video chat*, merupakan teknologi untuk melakukan interaksi audio dan video secara *real time* antara pengguna di lokasi yang berbeda. *Video chatting* biasanya dilakukan melalui perangkat komputer maupun Tablet atau smartphone (juga disebut telepon *video call*). *Video chatting* dapat berupa interaksi *point-to-point* (satu-satu), seperti FaceTime dan Skype, atau interaksi *multipoint* (satu-ke-banyak, atau banyak-ke-banyak), seperti dalam Google+ Hangouts. *Videochatting* sering disalah artikan dengan

video conference. *Videochatting* merujuk pada komunikasi video di antara dua orang individu *(point to point*), sedangkan *video conference* mengacu pada komunikasi video di antara 3 pihak atau lebih *(multipoint).*

2. Komunikasi daring asinkron (tak serempak) adalah komunikasi menggunakan perangkat komputer dan dilakukan secara tunda. Contoh komunikasi daring asinkron adalah *e-mail*, forum, rekaman simulasi visual, serta membaca dan menulis dokumen daring melalui *World Wide Web.*

Dalam pengiriman pesan elektronik ada hal penting berupa enkripsi data. Enkripsi adalah proses yang menyandikan pesan atau *file* sehingga hanya bisa dibaca oleh orang-orang tertentu. Enkripsi menggunakan algoritma untuk mengacak, atau mengenkripsi, data dan kemudian menggunakan kunci bagi pihak penerima untuk menguraikan, atau mendekripsi, informasi. Pesan yang terkandung dalam pesan terenkripsi disebut sebagai teks biasa. Dalam bentuknya yang terenkripsi dan tidak dapat dibaca, ini disebut sebagai *ciphertext.* Bentuk dasar enkripsi mungkin sesederhana mengganti huruf. Ketika kriptografi semakin maju, kriptografer menambahkan lebih banyak langkah, dan dekripsi menjadi lebih sulit. Roda dan roda gigi akan digabungkan untuk membuat sistem enkripsi yang kompleks. Algoritma komputer kini telah menggantikan enkripsi mekanis.

Latihan

Untuk memperdalam pemahaman Anda mengenai materi di atas, kerjakanlah latihan berikut!

1) Jelaskan pengertian audit sistem informasi!
2) Jelaskan yang dimaksud dengan kontrol keamanan logis!
3) Jelaskan pengertian keamanan sistem informasi!

Petunjuk Jawaban Latihan

1) Audit sistem informasi merupakan suatu proses pengumpulan data dan evaluasi bukti untuk menetapkan apakah suatu sistem aplikasi komputer sudah diterapkan dan menerapkan sistem pengendalian internal yang sudah sepadan, apakah seluruh aktiva dilindungi dengan baik atau disalah gunakan dan juga terjamin integritas data, keandalan dan juga efektivitas serta efisiensi penyelenggaraan informasi berbasis komputer.
2) Kontrol keamanan logis adalah kontrol yang membatasi kapabilitas akses pengguna sistem dan mencegah pengguna yang tidak berwenang mengakses

sistem. Kontrol keamanan logis ada di dalam sistem operasi, sistem manajemen *database*, program aplikasi, atau ketiganya.

3) Sistem keamanan sistem informasi bisa diartikan sebagai kebijakan, prosedur, dan pengukuran teknis yang digunakan untuk mencegah akses yang tidak sah, perubahan program, pencurian, atau kerusakan fisik terhadap sistem informasi.

Rangkuman

1. Tujuan audit sistem informasi. untuk menetapkan apakah sistem informasi melindungi aset perusahaan, menjaga integritas data yang disimpan dan dikomunikasikan, mendukung tujuan perusahaan secara efektif, dan beroperasi secara efisien.
2. Beberapa perubahan mendasar dari sistem manual ke sistem berbasis komputer sebagai berikut. sistem informasi sering kali jauh lebih kompleks daripada sistem manual, sistem informasi memiliki kemampuan memproses data dalam jumlah besar, sistem informasi menyimpan data dalam bentuk elektronik dan sistem informasi memproses data secara otomatis.
3. Saat ini sistem terdapat beberapa posisi yang berhubungan dengan sistem informasi seperti *Programmer, Web Developer, Computer Systems Engineer, Database Administrator, Software Quality Assurance (QA), Business Intelligence Analyst,* Analis sistem, Manajer Sistem Informasi, CIO, CSO, CPO, CKO dan *Network Administrator*.
4. Terdapat dua jenis komunikasi daring yaitu komunikasi daring sinkron (serempak dan komunikasi daring asinkron (tak serempak).
5. Pengendalian pada sistem informasi secara umum diklasifikasikan menjadi dua bagian yaitu pengendalian umum dan pengendalian aplikasi enkripsi.

Tes Formatif 1

Pilihlah satu jawaban yang paling tepat!

1) Fungsi audit sistem informasi perusahaan adalah agar sistem informasi dapat ....
   A. digunakan, dikendalikan, dan diandalkan
   B. diperbaharui
   C. dikembangkan di masa depan
   D. ditelusuri penggunaannya

2) Enkripsi merupakan salah satu bagian dari perlindungan data dengan cara ....
   A. menyandikan pesan atau *file* sehingga hanya bisa dibaca oleh orang-orang tertentu
   B. merubah pesan atau *file* sehingga hanya bisa dibaca oleh orang-orang tertentu
   C. mengirimkan pesan atau *file* sehingga hanya bisa dibaca oleh orang-orang tertentu
   D. mendistribusikan pesan atau *file* sehingga hanya bisa dibaca oleh orang-orang tertentu

3) Sistem informasi dirancang agar setiap transaksi keuangan dapat terlacak. dengan kata lain, jejak audit harus ada yang dapat ....
   A. memilih dari mana setiap transaksi berasal dan bagaimana prosesnya
   B. menghentikan dari mana setiap transaksi berasal dan bagaimana prosesnya
   C. menentukan dari mana setiap transaksi berasal dan bagaimana prosesnya
   D. menghindari dari mana setiap transaksi berasal dan bagaimana prosesnya

4) Proses audit sistem informasi yang berhubungan dengan perangkat keras fokus pada 4 hal yaitu, *kecuali* ....
   A. efektivitas dan efisiensi penggunaan aset perangkat keras.
   B. sistem keamanan sebagai perlindungan aset perangkat keras
   C. ketersediaan penggunaan perangkat keras
   D. ketersediaan penggunaan perangkat fisik

5) Berikut ini adalah tahapan-tahapan yang harus dilakukan untuk melindungi keamanan data yang berhubungan dengan perangkat keras, *kecuali* ....
   A. perencanaan, yaitu kegiatan membuat rencana semua kegiatan yang dilakukan selama kegiatan audit sistem informasi
   B. *acquisistion* adalah kegiatan menganalisis sumber perangkat keras yang digunakan oleh perusahaan untuk mendukung sistem informasi yang digunakan oleh perusahaan
   C. *implementation* adalah kegiatan memahami dan mengawasi instalasi perangkat keras yang digunakan untuk mendukung sistem informasi perusahaan
   D. *maintenance* adalah kegiatan memahami proses pengadaan perangkat keras yang digunakan untuk mendukung sistem informasi

6) Audit bertujuan untuk menetapkan, apakah sistem informasi ....
   A. melindungi aset perusahaan, menjaga integritas data yang disimpan dan dikomunikasikan, mendukung tujuan perusahaan secara efektif, dan beroperasi secara efisien
   B. menilai aset perusahaan, integritas data yang disimpan dan dikomunikasikan, mendukung tujuan perusahaan secara efektif, dan beroperasi secara efisien
   C. mengevaluasi aset perusahaan, integritas data yang disimpan dan dikomunikasikan, mendukung tujuan perusahaan secara efektif, dan beroperasi secara efisien
   D. sistem informasi aset perusahaan, dapat menjaga integritas data yang disimpan dan dikomunikasikan, mendukung tujuan perusahaan secara efektif, dan beroperasi secara efisien

7) Kontrol keamanan logis adalah ....
   A. perlindungan keamanan atas sistem komputasi secara memadai dari akses yang tidak sah dan kerusakan yang tidak disengaja atau disengaja atau perubahan program perangkat lunak sistem, program aplikasi, dan data
   B. perencanaan keamanan atas sistem komputasi secara memadai dari akses yang tidak sah dan kerusakan yang tidak disengaja atau disengaja atau perubahan program perangkat lunak sistem, program aplikasi, dan data.
   C. penilaian keamanan atas sistem komputasi secara memadai dari akses yang tidak sah dan kerusakan yang tidak disengaja atau disengaja atau perubahan program perangkat lunak sistem, program aplikasi, dan data.
   D. evaluasi keamanan atas sistem komputasi secara memadai dari akses yang tidak sah dan kerusakan yang tidak disengaja atau disengaja atau perubahan program perangkat lunak sistem, program aplikasi, dan data.

8) Pengendalian aplikasi atau sistem informasi, baik manual dan terkomputerisasi, dalam aplikasi bisnis bertujuan untuk ....
   A. merencanakan data tersebut diproses secara lengkap, akurat, dan tepat waktu
   B. memastikan data tersebut diproses secara lengkap, akurat, dan tepat waktu
   C. menyimpan data tersebut diproses secara lengkap, akurat, dan tepat waktu
   D. mengevaluasi data tersebut diproses secara lengkap, akurat, dan tepat waktu

9) Dalam proses audit sistem informasi terkait dengan *hardware* harus meliputi beberapa proses …

A. perencanaan untuk memastikan semua proses mulai pengadaan perangkat lunak dari *supplier* hingga pembuangan perangkat keras ketika sudah habis umur ekonomisnya memenuhi standar keamanan perusahaan

B. implementasi untuk memastikan semua proses mulai pengadaan perangkat keras dari *supplier* hingga pembuangan perangkat keras ketika sudah habis umur ekonomisnya memenuhi standar keamanan perusahaan

C. *maintenance* untuk semua proses mulai pengadaan perangkat keras dari *supplier* hingga pembuangan perangkat keras ketika sudah habis umur ekonomisnya memenuhi standar keamanan perusahaan

D. evaluasi untuk memastikan semua proses mulai penjualan perangkat keras dari *supplier* hingga pembuangan perangkat keras ketika sudah habis umur ekonomisnya memenuhi standar keamanan perusahaan

10) Proses audit sering mengambil posisi yang cukup ketergantungan pada kontrol di sekitar komputer yang berarti, yaitu dalam ....

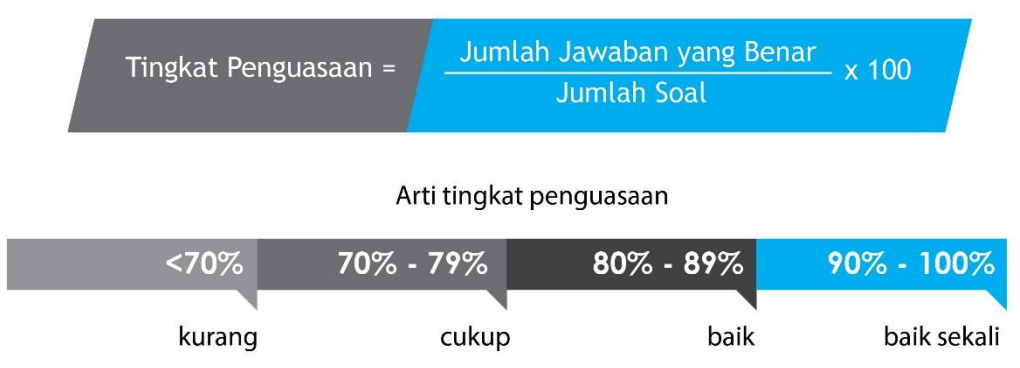
A. kontrol aplikasi atau sistem informasi karena auditor berkonsentrasi pada *input* dan *output* dari komputer, bukan apa yang terjadi pada komputer.

B. evaluasi aplikasi atau sistem informasi karena auditor berkonsentrasi pada *input* dan *output* dari komputer, bukan apa yang terjadi pada komputer.

C. kontrol aplikasi atau sistem informasi karena pengguna berkonsentrasi pada *input* dan *output* dari komputer, bukan apa yang terjadi pada komputer

D. kontrol aplikasi atau sistem informasi karena manajemen berkonsentrasi pada *input* dan *output* dari komputer, bukan apa yang terjadi pada komputer.

Cocokkanlah jawaban Anda dengan Kunci Jawaban Tes Formatif 1 yang terdapat di bagian akhir modul ini. Hitunglah jawaban yang benar. Kemudian, gunakan rumus berikut untuk mengetahui tingkat penguasaan Anda terhadap materi Kegiatan Belajar 1.



Apabila mencapai tingkat penguasaan 80% atau lebih, Anda dapat meneruskan dengan Kegiatan Belajar 2. **Bagus!** Jika masih di bawah 80%, Anda harus mengulangi materi Kegiatan Belajar 1, terutama bagian yang belum dikuasai.

Kegiatan Belajar 2

Teknologi dan Audit

Sebelum kita mulai membahas audit dan pengendalian sistem komputer, kita harus memiliki pemahaman yang sama tentang istilah dan proses yang digunakan dalam sistem informasi.

1. Perangkat keras, terdiri dari komponen-komponen yang secara fisik dapat disentuh dan dimanipulasi. Prinsip di antara komponen tersebut adalah:
   a. CPU, *Central Processing Unit* adalah jantung dari komputer. Merupakan unit logika yang menangani pemrosesan aritmatika semua perhitungan.
   b. *Periferal*, perangkat *periferal* adalah perangkat yang terhubung ke CPU untuk *troubleshooting*, yang biasanya berupa *input* dan *output*. Ini termasuk:
      Terminal
      Printer
      Perangkat penyimpanan *mobile* seperti *flashdisk*, *harddisk* eksternal.
2. Memori, berbentuk chip silikon di komputer modern yang mampu menyimpan informasi. Memori biasanya diukur dengan jumlah *byte data* yang dapat disimpan dalam memori pada satu waktu. Dua jenis memori utama biasanya mengacu pada komputer: memori pemrosesan dan memori penyimpanan. Memori pemrosesan sering disebut sebagai *Random Acces Memory* (RAM) atau memori sementara. Jumlah RAM yang tersedia di komputer biasanya dinyatakan dalam *megabyte* hingga *terabyte*. Semakin banyak RAM yang digunakan komputer, semakin banyak aplikasi yang dapat diproses secara bersamaan, sehingga memungkinkan pengguna untuk beralih dari satu aplikasi ke aplikasi lain tanpa harus keluar dari aplikasi sebelumnya. Setelah komputer dimatikan atau daya terputus, sebagian besar informasi yang berada di RAM tidak disimpan, maka ada istilah memori sementara. Banyak aplikasi dapat disimpan di RAM. Misalnya, ada beberapa perangkat lunak keamanan yang berada dalam RAM dan mengharuskan pengguna untuk memasukkan kata sandi sebelum komputer dapat melanjutkan proses inisialisasi.

   Perangkat lunak ini dapat mencegah pengguna yang tidak sah untuk menginisialisasi komputer dengan menempatkan disket inisialisasi ke dalam *drive* eksternal. Pengguna yang tidak sah dapat menggunakan teknik ini untuk menginisialisasi komputer, menghindari aplikasi keamanan masuk yang kurang

baik yang tidak ada di RAM, lalu mengakses *harddrive* dari *drive* eksternal. Sayangnya, banyak virus komputer juga dapat berada di RAM. Setelah virus tinggal di RAM komputer, mereka dapat menginfeksi komputer lain dan server *file* dengan menginfeksi memori penyimpanan mengacu pada jumlah *byte* data yang dapat disimpan di *harddrive* komputer. Tidak seperti RAM, memori penyimpanan tetap ada meskipun setelah daya dimatikan. Jadi, memori penyimpanan terkadang disebut sebagai memori permanen. Namun, itu permanen hanya sampai informasi tersebut benar-benar dihapus.

Perhatikan bahwa tindakan menghapus *file* tidak benar-benar menghapus data. Ini hanya menghapus referensi lokasi *file*. Data tetap berada di media penyimpanan sampai ditimpa. Karena sebagian besar komputer menyimpan data secara berurutan, diperlukan beberapa minggu, bulan, atau tahun untuk memperbaharui *file* yang sebelumnya dihapus, bergantung pada jumlah data yang telah disimpan dan dihapus serta ukuran media penyimpanan. Banyak organisasi memiliki program penyimpanan data cadangan untuk membantu memastikan pemulihan data jika terjadi bencana. Bergantung pada frekuensi rotasi dan periode penyimpanan media cadangan, data dapat diperbanyak tanpa batas. Untuk alasan ini, terutama saat bekerja dengan informasi yang sangat sensitif, rahasia, atau sangat rahasia, sangat penting untuk mengamankan akses ke media penyimpanan komputer secara memadai.

3. *Mainframe*. Komputer *mainframe* adalah komputer besar (secara fisik maupun daya) yang digunakan oleh perusahaan untuk melakukan pemrosesan volume besar dan komputasi terkonsentrasi.
4. Mini komputer, secara fisik lebih kecil dari *mainframe*, meskipun kekuatan mini komputer melebihi *mainframe* saat ini.
5. Mikro komputer, komputer mikro adalah komputer kecil secara fisik dengan daya pemrosesan dan penyimpanan terbatas. Karena itu, kekuatan dan kapasitas mikro saat ini setara dengan *mainframe* lima tahun lalu.
6. Penyimpanan Data disimpan dalam berbagai bentuk baik untuk penyimpanan permanen maupun sementara:
    a. *Bit*, digit biner, satu dan nol
    b. *Byte*, koleksi bits yang menyusun karakter individu
    c. *Disk*, perangkat penyimpanan berkapasitas besar yang berisi data hingga ukuran *terabyte*
    d. *Memory*
7. Komunikasi, untuk memaksimalkan potensi penggunaan informasi yang efektif pada komputer, komputer yang terisolasi harus dapat berkomunikasi dan berbagi data, program, dan perangkat keras.
8. Terminal, perangkat jarak jauh memungkinkan *input* dan *output* ke dan dari komputer data dan program.

9. Modem, modulator / *De-Modulator*, yang menerjemahkan sinyal komputer digital menjadi sinyal analog untuk kabel telepon dan menerjemahkannya kembali di ujung lain. Bagian dari modem ini adalah sebagai berikut.
   a. *Multiplexer*, menggabungkan sinyal dari berbagai perangkat untuk memaksimalkan pemanfaatan jalur komunikasi yang mahal.
   b. Kabel, kabel logam, biasanya tembaga, yang dapat membawa sinyal antar komputer. Ini mungkin datang dalam bentuk "pasangan terpilin", di mana dua atau lebih kabel dirangkai dalam selongsong plastik, atau dalam bentuk koaksial, dimana kabel dipasang di dalam jalinan logam dengan cara yang sama seperti kabel antena televisi.
   c. Serat optik, ini terdiri dari untaian halus *fiberglass* atau filamen plastik yang membawa sinyal cahaya tanpa perlu isolasi listrik. Mereka memiliki kapasitas dan kecepatan transfer yang sangat tinggi tetapi mahal.
   d. *Microwave*, bentuk komunikasi ini melibatkan pengiriman sinyal berkekuatan tinggi dari pemancar ke penerima. Mereka bekerja berdasarkan garis pandang langsung tetapi tidak memerlukan kabel.
10. *Input* ke sistem komputer telah berkembang pesat selama bertahun-tahun. Auditor SI kadang-kadang masih akan menemui beberapa jenis perangkat *input.*
   a. *Punch card* adalah salah satu media *input* dan *output* pertama dan terdiri dari lembaran karton, berukuran 8 × 4 inci dengan 80 kolom, di mana lubang persegi panjang dapat dilubangi dalam kombinasi untuk mewakili karakter numerik, alfabet, dan khusus.
   b. *Keyboad* /Papan Ketik, perangkat *input* paling umum saat ini (meskipun itu berubah). Kebanyakan *keyboard* masih didasarkan pada desain *keyboard* QWERTY juru ketik asli.
   c. *Mouse*, perangkat penunjuk elektromekanis yang digunakan untuk memasukkan instruksi secara *real time.*
   d. Pemindai, perangkat optik yang dapat memindai gambar menjadi bentuk digital yang dapat dibaca komputer. Perangkat ini dapat digunakan bersama perangkat lunak OCR (pengenalan karakter optik) untuk memungkinkan komputer menginterpretasikan gambar data menjadi data karakter.
   e. Kode batang / *barcode*, *barcode* adalah gambar yang terdiri dari serangkaian garis hitam dan putih paralel yang, ketika dipindai, menyampaikan informasi tentang suatu produk. Kode batang dibaca oleh pemindai optik khusus. Setelah perangkat pemindai ditempatkan di seberang kode batang, perangkat akan segera memproses data yang ada di dalamnya, biasanya harga produk tempat kode batang dicetak. Bentuk paling umum dari kode batang adalah kode produk universal (UPC), yang pertama kali diperkenalkan pada tahun 1970-an untuk digunakan di toko bahan makanan. *Barcode* adalah bagian penting dari perekonomian.

Barcode adalah bagian rutin dari transaksi komersial, muncul di hampir setiap produk yang tersedia untuk dibeli di toko. Ide di balik *barcode* cukup sederhana. Setiap item berbeda memiliki nomor unik yang tercetak di atasnya yang dapat dibaca dan dikenali oleh perangkat pemindai. Hal ini memungkinkan untuk mengotomatiskan transfer informasi produk, seperti harganya, dari produk ke sistem elektronik seperti mesin kasir. *Barcode* dapat dibaca dengan berbagai jenis teknologi. Pemindai secara khusus diprogram untuk mentransfer data yang disimpan oleh kode batang ke program aplikasi, menyediakan akses cepat ke banyak informasi. Pemindai antarmuka yang terhubung ke komputer mengirimkan informasi kode batang seolah-olah itu dimasukkan ke *keyboard*.

Barcode lebih dari sekadar memberikan harga dan detail dasar lainnya tentang suatu produk. *Barcode* membantu menghemat waktu, menghilangkan kemungkinan kesalahan manusia, dan umumnya membuat perusahaan lebih efisien. Ketika *barcode* ditautkan ke *database*, *barcode* memungkinkan pengecer melacak inventaris, memungkinkan mereka dengan mudah memantau tren dalam kebiasaan konsumen, memesan lebih banyak stok, dan menyesuaikan harga. *Barcode* juga dapat digunakan dalam aplikasi lain seperti industri perawatan kesehatan, di mana mereka digunakan untuk mengidentifikasi pasien dan catatan pasien. Mereka juga dapat membantu menyebarkan informasi penting lebih lanjut seperti riwayat medis dan obat resep serta alergi. Banyak industri lain juga memanfaatkan *barcode*. Teknologi ini dikenal dapat meningkatkan efisiensi di berbagai industri, termasuk layanan pos, perjalanan, dan pariwisata (persewaan mobil, koper), dan hiburan (tiket bioskop dan teater, taman hiburan).

f. QR *Code* atau *quick respons code* adalah kode yang dapat dibaca kamera pada *smartphone* yang terdiri dari larik kotak hitam dan putih, biasanya digunakan untuk menyimpan URL atau informasi lain. QR *Code* merupakan pengembangan dari barcode yang bisa menangkap data tidak hanya angka seperti di *barcode* tapi lebih dari itu seperti gambar, simbol dan lain-lain. Kode QR adalah suatu jenis kode matriks atau kode batang dua dimensi yang dikembangkan oleh *Denso Wave*, sebuah divisi *Denso Corporation* yang merupakan sebuah perusahaan Jepang dan dipublikasikan pada tahun 1994 dengan fungsionalitas utama yaitu dapat dengan mudah dibaca oleh pemindai QR merupakan singkatan dari *quick response* atau respons cepat, yang sesuai dengan tujuannya adalah untuk menyampaikan informasi dengan cepat dan mendapatkan respons yang cepat pula.

Berbeda dengan kode batang, yang hanya menyimpan informasi secara horizontal, kode QR mampu menyimpan informasi secara horizontal dan vertikal, oleh karena itu secara otomatis Kode QR dapat menampung informasi yang lebih banyak daripada kode batang. Awalnya kode QR digunakan untuk pelacakan kendaraan bagian di manufaktur, namun kini kode QR digunakan dalam konteks yang lebih luas, termasuk aplikasi komersial dan kemudahan pelacakan aplikasi berorientasi yang ditujukan untuk pengguna telepon seluler. Di Jepang, penggunaan kode QR sangat populer, hampir semua jenis ponsel di Jepang bisa membaca kode QR sebab sebagian besar pengusaha di sana telah memilih kode QR sebagai alat tambahan dalam program promosi produknya, baik yang bergerak dalam perdagangan maupun dalam bidang jasa. Pada umumnya kode QR digunakan untuk menanamkan informasi alamat situs suatu perusahaan. Di Indonesia, kode QR pertama kali diperkenalkan oleh *KOMPAS*. Dengan adanya kode QR pada koran harian di Indonesia ini, pembaca mampu mengakses berita melalui ponselnya bahkan bisa memberi masukan atau opini ke reporter atau editor surat kabar tersebut.

g. RFID atau *Radio Frequency Identification* adalah teknologi yang menggunakan gelombang radio untuk secara pasif mengidentifikasi objek yang diberi tag. Teknologi ini digunakan dalam beberapa aplikasi komersial dan industri, untuk melacak item di sepanjang rantai pasokan untuk melacak item yang diperiksa dari perpustakaan. *Radio Frequency Identification* (RFID) adalah jenis teknologi nirkabel pasif yang memungkinkan untuk melacak atau mencocokkan item atau individu. Sistem ini memiliki dua bagian dasar *tag* dan *reader*. *Reader* mengeluarkan gelombang radio dan mendapatkan sinyal kembali dari *tag* RFID, sedangkan *tag* menggunakan gelombang radio untuk mengkomunikasikan identitasnya dan informasi lainnya. Teknologi ini telah disetujui sejak sebelum tahun 1970-an tetapi telah menjadi lebih umum dalam beberapa tahun terakhir karena penggunaannya semakin luas seperti manajemen rantai pasok global dan *microchipping* hewan peliharaan.

h. Pengenal suara atau *voice recognition*. *Voice recognition* memungkinkan konsumen untuk melakukan banyak tugas dengan berbicara langsung ke *Google Home* , Amazon Alexa atau teknologi pengenal suara lainnya. Dengan menggunakan *machine learning* dan algoritma canggih, teknologi pengenal suara dapat dengan cepat mengubah pekerjaan lisan Anda menjadi teks tertulis. Di masa depan *input* komputer di mana pengguna komputer, *programmer*, atau auditor hanya mendikte ke mikrofon dan komputer merespons dengan tepat.

11. *Output* seperti halnya *input*, *output* berubah dengan cepat. Pada masa komputasi paling awal, *output* biasanya terdiri atas kertas, layar atau komputer lain yang akan di proses oleh komputer lainnya .
    a. Monitor, perangkat keluaran komputer yang paling umum yang menciptakan tampilan visual dengan menggunakan mana pengguna dapat melihat data yang diproses. Monitor tersedia dalam berbagai ukuran dan resolusi. Jenis umum monitor adalah *Cathode Ray Tube* - ini menggunakan titik berpendar untuk menghasilkan piksel yang merupakan gambar yang ditampilkan layar panel datar, memanfaatkan kristal cair atau plasma untuk menghasilkan keluaran. Cahaya dilewatkan melalui kristal cair untuk menghasilkan piksel. Semua monitor bergantung pada kartu video, yang ditempatkan di *motherboard* komputer atau di slot ekspansi khusus. Kartu video memilah data komputer menjadi detail gambar yang kemudian dapat ditampilkan oleh monitor.
    b. Printer, perangkat ini menghasilkan versi *hardcopy* dari data yang diproses, seperti dokumen dan foto. Komputer mengirimkan data gambar ke printer, yang kemudian secara fisik membuat ulang gambar tersebut, biasanya di atas kertas. Jenis printer InkJet bekerja dengan menyemprotkan titik-titik kecil tinta ke permukaan untuk membentuk gambar dan laser, jenis ini menggunakan drum toner yang menggulung pigmen bermagnet, dan kemudian mentransfer pigmen tersebut ke permukaan. Dan terakhir dot matrix, printer dot matrix menggunakan *print head* untuk mengatur gambar pada permukaan, menggunakan pita tinta. Printer ini biasanya digunakan antara tahun 1980 dan
    c. *Speaker*, *speaker* terpasang ke komputer untuk memfasilitasi keluaran suara, kartu suara diperlukan di komputer agar *speaker* berfungsi. Berbagai jenis *speaker* berkisar dari perangkat *output* dua *speaker* yang sederhana hingga unit multi saluran *surround sound.*
    d. *Headset*, ini adalah kombinasi *speaker* dan mikrofon. Ini sebagian besar digunakan oleh para *gamer*, dan juga merupakan alat yang hebat untuk berkomunikasi dengan keluarga dan teman melalui internet menggunakan beberapa program VOIP atau lainnya.
    e. Proyektor, ini adalah perangkat layar yang memproyeksikan gambar buatan komputer ke permukaan lain: biasanya semacam papan tulis atau dinding. Komputer mengirimkan data gambar ke kartu videonya, yang kemudian mengirimkan gambar video ke proyektor. Ini paling sering digunakan untuk presentasi, atau untuk melihat video.
    f. *Plotter*, ini menghasilkan salinan cetak dari desain yang digambarkan secara digital. Desain dikirim ke *plotter* melalui kartu grafis, dan desain tersebut dibentuk dengan menggunakan pena. Ini umumnya digunakan dengan aplikasi teknik, dan pada dasarnya menggambar gambar tertentu

menggunakan serangkaian garis lurus. Kertas masih merupakan media keluaran yang populer, dan merupakan bentuk alat tulis berkelanjutan, bentuk lembaran potongan, atau stok bisnis pracetak seperti faktur atau instrumen yang dapat dinegosiasikan seperti cek.

12. *Online system, real time system* dan *batch system*

Batch processing adalah suatu model pengolahan data, dengan menghimpun data terlebih dahulu, dan diatur pengelompokan datanya dalam kelompok-kelompok yang disebut *batch*. Tiap *batch* ditandai dengan identitas tertentu, serta informasi mengenai data-data yang terdapat dalam *batch* tersebut. Setelah data-data tersebut terkumpul dalam jumlah tertentu, data-data tersebut akan langsung diproses. Contoh dari penggunaan *batch processing* adalah e-mail dan transaksi *batch processing*. Dalam suatu sistem *batch processing*, transaksi secara individual dientri melalui peralatan terminal, dilakukan validasi tertentu, dan ditambahkan ke *transaction file* yang berisi transaksi lain, dan kemudian dientri ke dalam sistem secara periodik. Di waktu kemudian, selama siklus pengolahan berikutnya, *transaction file* dapat divalidasi lebih lanjut dan kemudian digunakan untuk meng-*up date* master *file* yang berkaitan.

Tidak diperlukan interaksi pengguna saat *batch processing* berlangsung. Ini membedakan *batch processing* dari proses transaksi, yang melibatkan transaksi pengolahan satu per satu dan membutuhkan interaksi pengguna. Sementara *batch processing* dapat dilakukan setiap saat, itu sangat cocok untuk mengakhiri siklus pengolahan, seperti untuk memproses laporan bank pada akhir hari, atau menghasilkan gaji bulanan atau dua mingguan. *Batch processing* adalah kegiatan memprosesan satu set besar data dengan cara tertentu, secara otomatis, tanpa perlu campur tangan pengguna. Data pertama dikumpulkan, selama hari kerja, misalnya, dan kemudian *batch processing*, sehingga semua data yang dikumpulkan diolah dalam satu bagian. Hal ini bisa terjadi pada akhir hari kerja, misalnya, ketika kapasitas komputasi yang tidak diperlukan untuk tugas-tugas lainnya.

Keuntungan dari proses ini adalah dimungkinkan untuk melakukan tugas-tugas yang berulang-ulang pada sejumlah besar potongan-potongan data dengan cepat tanpa perlu pengguna untuk memonitor. Kemudian ada juga istilah pengolahan interaktif atau *online* yaitu data langsung diproses saat itu dimasukkan, pengguna biasanya hanya harus menunggu waktu yang singkat untuk jawaban. (ex. *game*, pengolah kata, sistem pemesanan). Pengolahan interaktif atau *online* mengharuskan pengguna untuk memasok *input*. Keuntungan sistem ini adalah: interaktif atau pengolahan *online* memungkinkan pengguna untuk *input* data dan mendapatkan hasil dari pengolahan data yang segera. Selain itu ada pengolahan *real time* dimana *real time* adalah bagian dari proses interaktif atau *online*.

Sementara *real time processing* adalah *input* terus menerus, secara otomatis diperoleh dari sensor, misalnya, yang segera diproses untuk menrespon masukan

dalam waktu sesedikit mungkin. Setelah sistem ini selesai menanggapi membaca set berikutnya *input* data segera memproses itu. Sistem ini tidak memerlukan pengguna untuk mengontrolnya, sistem bekerja secara otomatis. Keuntungan dari sistem ini adalah setiap kali ada reaksi cepat diperlukan karena beberapa jenis perubahan, pengolahan *real time* dapat mengambil tindakan tanpa perlu pengguna atau waktu proses yang lama terlebih dahulu.

Sedangkan *online processing* adalah sebuah sistem yang mengaktifkan semua periferal sebagai pemasok data, dalam kendali komputer induk. Informasi-informasi yang muncul merupakan refleksi dari kondisi data yang paling mutakhir, karena setiap perkembangan data baru akan terus melakukan *update* ke data induk. Salah satu contoh penggunaan *online processing* adalah transaksi *online*. Dalam sistem pengolahan *online*, transaksi secara individual dientri melalui peralatan terminal, divalidasi dan digunakan untuk melakukan update dengan segera kedalam *file* komputer. Hasil pengolahan ini kemudian tersedia segera untuk permintaan keterangan atau laporan.

13. Jenis sistem komputer

Secara umum sistem komputer terbagi 2 yaitu sistem operasi dan sistem aplikasi. Dibawah ini penjelasan rinci dari kedua sistem tersebut.

a. Sistem operasi adalah sistem yang mengelola unit pemrosesan pusat atau CPU yang terhubung ke berbagai perangkat periferal yang membantu dalam menyimpan, mengakses, dan mengirimkan data dan juga dalam produksi keluaran informasi. Contoh perangkat periferal termasuk drive disk eksternal, drive CD-ROM dan CD-RW tunggal, beberapa drive CD-ROM (terkadang disebut "*jukebox*"), *drive* pita magnetik, paket *disk*, printer, *router*, *gateway*, *gateway* pengontrol, visual monitor, *keyboard*, terminal, dan lainnya. Perangkat ini secara kolektif disebut sebagai perangkat keras komputer. Sistem operasi juga adalah program yang diperlukan untuk membuat perangkat keras berfungsi. Perangkat keras tersebut biasanya terdapat ke komputer selama proses pembuatan.

   Sistem operasi biasanya mencakup bermacam-macam program utilitas yang membantu dalam fungsi, pemeliharaan, dan keamanan berbagai perangkat keras. Sistem operasi dan utilitas secara kolektif disebut sebagai perangkat lunak sistem. Contoh sistem operasi umum termasuk DOS, Windows, OS / 2, NetWare, OSX, Unix, VMS, dan OS / 390.23 Fitur tertentu dalam perangkat lunak sistem dapat disesuaikan oleh pembeli. Misalnya, sistem operasi yang paling canggih memiliki fitur kontrol akses sistem yang memungkinkan pembeli untuk melindungi sistem secara memadai dari akses yang tidak sah. Produsen biasanya menetapkan parameter kontrol akses sistem untuk memungkinkan akses yang hampir tidak terbatas selama instalasi awal. Ini diperlukan agar pengguna yang melakukan penginstalan awal dapat mengatur pengguna lain,

mengkonfigurasi sistem, dan menyesuaikan pengaturan parameter sistem yang tersedia.

Meskipun pabrikan komputer biasanya membantu dalam pemasangan awal sistem yang kompleks, mereka cenderung lebih mengutamakan membuat sistem beroperasi daripada sistem keamanan karena sistem keamanan merupakan fitur tambahan dari sebuah sistem operasi. Faktanya, banyak teknisi vendor biasanya membuat identifikasi pengguna (ID) untuk diri mereka sendiri, yang memiliki hak yang sama seperti administrator keamanan sistem. Seringkali mereka tidak menghapus ID pengguna setelah mereka menyelesaikan instalasi. Akibatnya, organisasi menghadapi risiko akses tidak sah oleh teknisi pemasangan. Inilah salah satu alasan penting bagi auditor sistem informasi untuk dilibatkan dalam proyek implementasi sistem baru.

b. Program aplikasi dimana program aplikasi diperlukan untuk membuat CPU dan perangkat lunak sistem menjalankan fungsi bisnis. Banyak program aplikasi siap pakai dibangun untuk melakukan tugas umum seperti pengolah kata (misalnya, word, *spreadsheet* (misalnya, excel), dan analisis data (misalnya, *access*). Banyak aplikasi lain telah dibangun untuk menjalankan fungsi bisnis tertentu di berbagai industri (misalnya, aplikasi pinjaman dan deposito di lembaga keuangan, aplikasi kartu kredit di perusahaan penerbit kartu, aplikasi desain komputer di perusahaan manufaktur mobil dan pesawat, dan aplikasi pemrosesan klaim di perusahaan asuransi).

c. Beberapa aplikasi perencanaan sumber daya perusahaan (ERP/ *Enterprise Resource Planning*) ada yang membantu menjalankan fungsi bisnis umum seperti akuntansi keuangan, hutang dagang, sumber daya manusia, penggajian, manajemen aset tetap, dan sebagainya. Contoh aplikasi ERP ini termasuk PeopleSoft, SAP, Oracle, Baan, J. D. Edwards, dan Lawson. Jutaan aplikasi lain telah dikembangkan secara internal oleh perusahaan dan secara eksternal oleh vendor untuk menjalankan berbagai fungsi bisnis, beberapa di antaranya dalam berbagai bahasa. Masing-masing aplikasi ini mungkin atau mungkin tidak memiliki fitur kontrol yang dirancang untuk membantu mencegah akses tidak sah ke aplikasi tersebut. Untuk menilai kecukupan kontrol atas aplikasi ini, pengetahuan rinci tentang fitur kontrol yang tersedia dalam aplikasi tertentu yang saat ini digunakan dalam organisasi harus diperoleh.

d. Program aplikasi berbasis *cloud computing*. *Cloud Computing* merupakan gabungan pemanfaatan teknologi komputer (komputasi) dalam suatu jaringan dengan pengembangan berbasis internet (awan) yang mempunyai fungsi untuk menjalankan program atau aplikasi melalui komputer – komputer yang terkoneksi pada waktu yang sama, tetapi tak semua yang terkoneksi melalui internet menggunakan *cloud computing*. Teknologi

komputer berbasis sistem *cloud* ini merupakan sebuah teknologi yang menjadikan internet sebagai pusat server untuk mengelola data dan juga aplikasi pengguna. Teknologi ini mengizinkan para pengguna untuk menjalankan program tanpa instalasi dan mengizinkan pengguna untuk mengakses data pribadi mereka melalui komputer dengan akses internet. Berikut ini adalah beberapa aplikasi berbasis *cloud computing*

- Google drive. Layanan penyimpanan *online* yang dimiliki google. Diluncurkan pada tanggal 24 April 2012. Serta memberikan kapasitas penyimpanan sebesar 5GB kepada setiap penggunanya. Kapasitas tersebut dapat ditambahkan dengan melakukan pembayaran atau pembelian storage.
- Windows azure. Sistem operasi yang berbasis komputasi awan, dibuat oleh microsoft untuk mengembangkan dan mengatur aplikasi serta melayani sebuah jaringan global dari microsoft data centers. Windows azure yang mendukung berbagai macam bahasa dan alat pemrograman. Sistem operasi ini dirilis pada 1 Februari 2010.
- Yahoo.com, sebuah perusahaan internet multinasional yang berpusat di Sunnyvale, California, Amerika Serikat. Perusahaan ini terkenal karena portal *web*nya, serta mesin pencari (Yahoo! Search), Yahoo! Directory, Yahoo! Mail, Yahoo! News, Yahoo! Finance, Yahoo! Groups, Yahoo! Answers, situs dan layanan periklanan, peta daring, berbagi video, olahraga fantasi dan media sosialnya.
- *Evernote*, mungkin biasanya kita membuat catatan dalam microsoft word, tapi apakah kita harus membawa kemana-mana laptop atau PC untuk mencatat sesuatu? *Evernote* dapat membuat catatan atau notes, menyimpan beberapa artikel yang ditemukan ketika browsing, menyimpan ide-ide, dan ditambah lagi bisa di akses dengan PC, *smartphone*, ipad dan lainnya.
- Dropbox, dapat menyimpan dan membagikan *file*, berkolaborasi pada proyek, dan mewujudkan ide terbaik, baik saat bekerja sendiri atau sebagai bagian dari tim.
- *Skydrive*, layanan penyimpanan data milik microsoft yang berbasis *cloud* server. Dimana kita bisa ‘menitipkan’ data-data ke server microsoft dengan satu akun yang sama (*Windows Live ID*). Layanan ini setara dengan layanan lain semisal dropbox atau google drive.
- Scribd, sebuah *web*site yang berisikan berbagai macam dokumen / data yang menyatu dalam sebuah halaman *web* dengan menggunakan i-paper format.

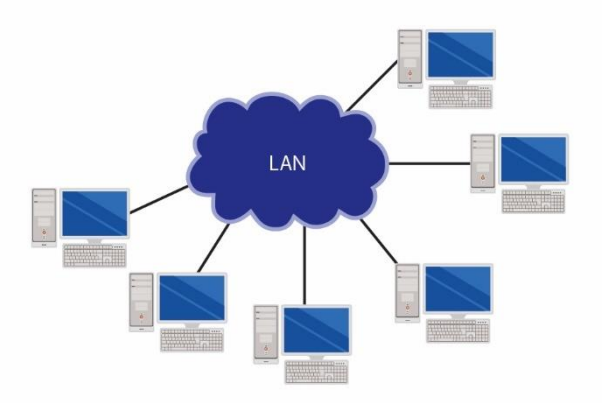
14. Jaringan komputer

Jaringan komputer adalah sekumpulan komputer yang terhubung. Komputer di jaringan disebut node. Koneksi antar komputer dapat dilakukan melalui

pemasangan kabel, paling umum kabel ethernet, atau kabel serat optik. Koneksi juga bisa nirkabel, Anda akan mendengar istilah wifi untuk menggambarkan informasi yang dikirim melalui gelombang radio. Komputer yang terhubung dapat berbagi sumber daya seperti akses ke internet, printer, server *file*, dan lainnya. Jaringan adalah koneksi multiguna, yang memungkinkan satu komputer melakukan lebih dari yang seharusnya tanpa koneksi apa pun

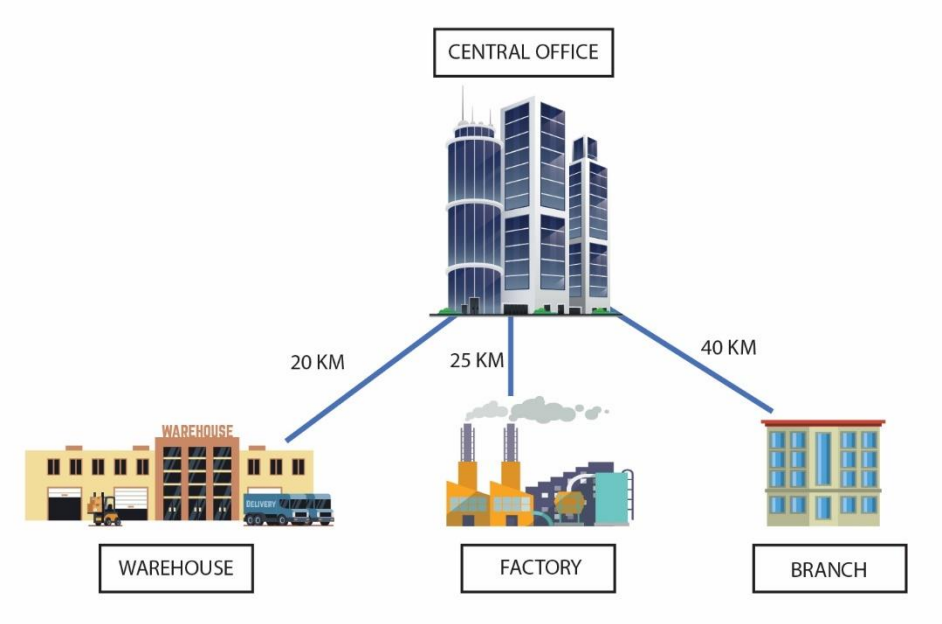
A. JENIS JARINGAN BERDASARKAN LUAS JANGKAUAN

1. ***Local Area Network*** **(LAN)** merupakan jaringan komputer yang sering digunakan untuk menghubungkan komputer-komputer pribadi dan *workstation* dalam suatu kantor suatu perusahaan atau pabrik- pabrik untuk memakai sumber daya (*resource*, misalnya printer) secara bersama-sama dan saling bertukar informasi yang masih dalam satu area, sebagai contoh dapat dilihat pada Gambar 1.1.



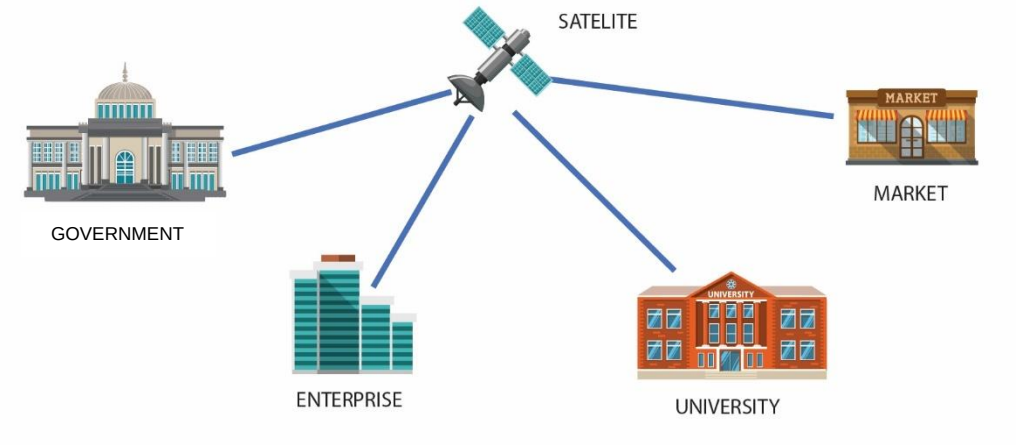
Gambar 1.1
Local Area Network (LAN)

2. ***Metropolitan Area Network*** **(MAN).** Hampir sama dengan LAN yang merupakan versi LAN yang berukuran lebih besar dan biasanya menggunakan teknologi yang sama dengan LAN. MAN dapat mencakup kantor- kantor perusahaan yang terletak berdekatan atau juga sebuah kota dan dapat di manfaatkan untuk keperluan pribadi (swasta) atau umum. MAN mampu menunjang daya dan suara, bahkan dapat berhubungan dengan jaringan Televisi Kabel. biasanya MAN digunakan dalam area 1 kota, bukan hanya satu lokasi saja, sebagai contoh dapat dilihat pada Gambar 1.2.



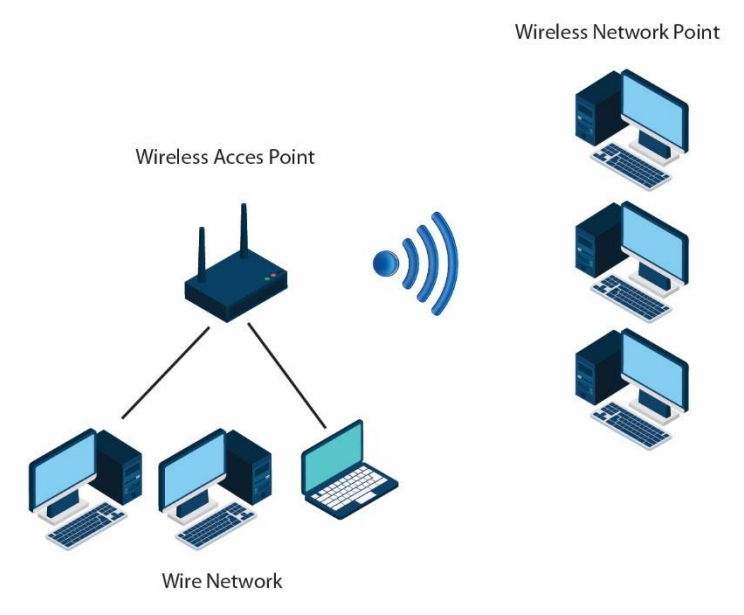
Gambar 1.2
Metropolitan Area Network (MAN)

3. ***Wide Area Network* (WAN)**, jaringan WAN merupakan jaringan yang mencakup daerah geografis yang lebih luas, seringkali mancakup sebuah negara bahkan antar benua. WAN terdiri dari kumpulan mesin-mesin yang bertujuan untuk menjalankan Program-program (Aplikasi) pemakai, bisa dikatakan jaringan WAN merupakan jaringan internet yang kita kenal saat ini, sebagai contoh dapat dilihat pada Gambar 1.3.



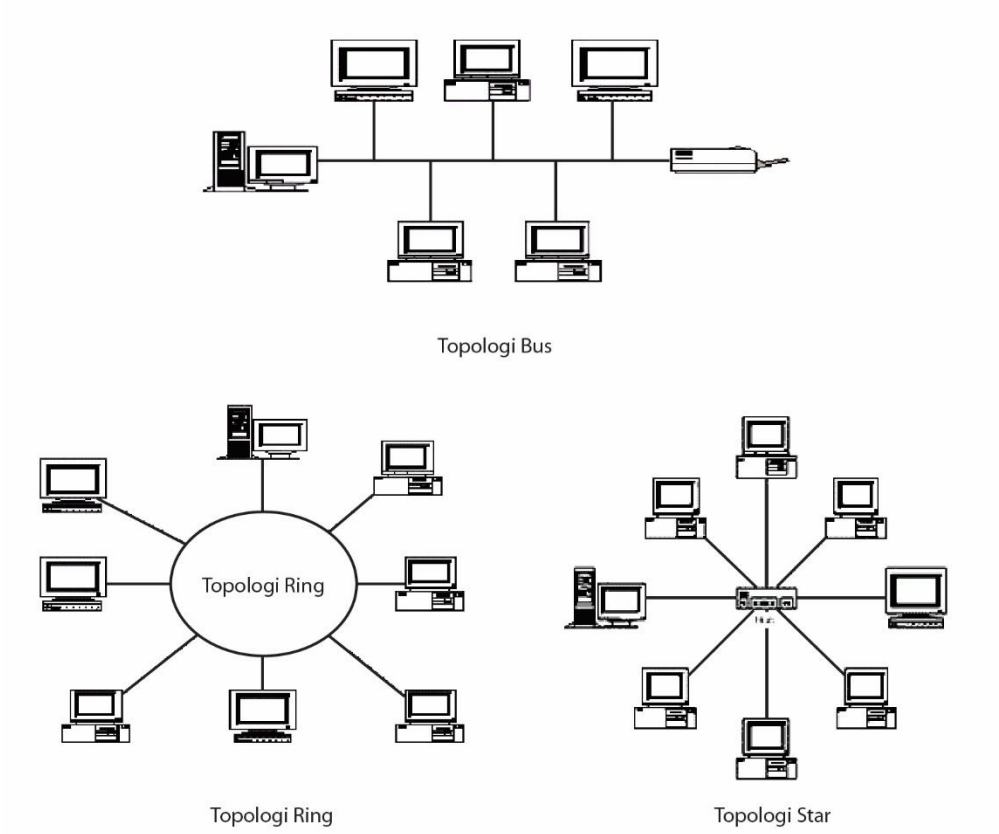
Gambar 1.3
Wide Area Network (WAN)

4. ***Wireless Local Area Network* (WLAN)**, jaringan nirkabel merupakan suatu solusi terhadap komunikasi yang tidak bisa dilakukan dengan jaringan menggunakan kabel. Saat ini jaringan tanpa kabel atau *wireless* sudah marak di gunakan dengan memanfaatkan jasa satelit dan mampu memberi kecepatan akses yang lebih cepat di bandingkan dengan jaringan yang menggunakan kabel. dengan adanya jaringan *wireless* memudahkan penggunaan *user* untuk mengakses data yang di inginkan di tempat-tempat yang tidak terjangkau oleh jaringan kabel, misal pada saat *mobile* / bepergian, sebagai contoh dapat dilihat pada Gambar 1.4.



Gambar 1.4
Wireless Local Area Network (WLAN)

5. ***Personal Area Network* (PAN)**, merupakan jaringan antara dua atau lebih sistem komputer yang berjarak tidak terlalu jauh. Biasanya jenis jaringan yang satu ini hanya berjarak 1 sampai 5 meter saja. Jenis jaringan ini sangat sering kita gunakan, misalnya pada saat kita menghubungkan komputer dengan HP, *headset* ataupun perangkat sejenis lainnya
6. **Topologi jaringan**, selain jenis jaringan komputer seperti yang telah dijelaskan di atas ada juga pengertian jaringan sebagai konfigurasi titik ke titik yang disebut sebagai topologi jaringan, seperti yang terlihat pada Gambar 1.5. Konfigurasi alternatif dapat berupa konfigurasi *multi drop* dengan beberapa terminal yang berbagi satu jalur. Jaringan dengan model ring tidak memiliki komputer pusat dimana setiap komputer *client* digolongkan sebagai "*node*" di jaringan, dan *Star Networks* memiliki satu komputer pusat yang mengoordinasikan semua komunikasi dalam jaringan.



Gambar 1.5
Jenis Topologi Jaringan

D. SISTEM KEAMANAN PADA JARINGAN KOMPUTER

Keamanan jaringan saat ini menjadi isu yang sangat penting dan terus berkembang. Beberapa kasus menyangkut keamanan sistem saat ini adalah perkembangan teknologi komputer, selain menimbulkan banyak manfaat juga memiliki banyak sisi buruk. Salah satunya adalah serangan terhadap sistem komputer yang terhubung ke internet. Sebagai akibat dari serangan itu, banyak sistem komputer atau jaringan yang terganggu bahkan menjadi rusak. Untuk menanggulangi hal tersebut, diperlukan sistem keamanan yang dapat menanggulangi dan mencegah kegiatan-kegiatan yang mungkin menyerang sistem jaringan kita. Dalam perkembangan teknologi dewasa ini, sebuah informasi menjadi sangat penting bagi sebuah organisasi. Informasi tersebut biasanya dapat diakses oleh para penggunanya. Akan tetapi, ada masalah baru yang berakibat dari keterbukaan akses tersebut. Masalah-masalah tersebut antara lain adalah sebagai berikut.

1. Pemeliharaan validitas dan integritas data atau informasi tersebut.
2. Jaminan ketersediaan informasi bagi pengguna yang berhak.
3. Pencegahan akses sistem dari yang tidak berhak.

4. Pencegahan akses informasi dari yang tidak berhak merupakan hal yang membahayakan jaringan.

Untuk menjamin keamanan dalam jaringan, perlu dilakukan perencanaan keamanan yang matang berdasarkan prosedur dan kebijakan dalam keamanan jaringan. Perencanaan tersebut akan membantu dalam hal-hal berikut ini.

1. Menentukan data atau informasi apa saja yang harus dilindungi.
2. Menentukan berapa besar biaya yang harus ditanamkan dalam melindunginya.
3. Menentukan siapa yang bertanggung jawab untuk menjalankan langkah-langkah yang diperlukan untuk melindungi bagian tersebut.

Dalam merencanakan suatu keamanan jaringan, ada beberapa metode yang dapat diterapkan. Metode-metode tersebut adalah sebagai berikut.

1. Pembatasan akses pada suatu jaringan, ada 3 konsep yang ada dalam pembatasan akses jaringan, yakni sebagai berikut.
   a. *Internal Password, Authentication Password* yang baik menjadi penting dan sederhana dalam keamanan suatu jaringan. Kebanyakan masalah dalam keamanan jaringan disebabkan karena *password* yang buruk. Cara yang tepat antara lain dengan menggunakan *shadow password* dan menonaktifkan TFTP.
   b. *Server based password authentication* yaitu perlindungan server dengan menguji validitas *password* yang dimasukkan.
   c. *Firewall* dan *routing control* untuk *firewall* akan dijelaskan pada bagian selanjutnya.
2. Menggunakan metode enkripsi tertentu dasar enkripsi cukup sederhana. Pengirim menjalankan fungsi enkripsi pada pesan *plaintext*, *ciphertext* yang dihasilkan kemudian dikirimkan lewat jaringan, dan penerima menjalankan fungsi deskripsi (*decryption*) untuk mendapatkan *plaintext* semula. Proses enkripsi/dekripsi tergantung pada kunci (*key*) rahasia yang hanya diketahui oleh pengirim dan penerima. Ketika kunci dan enkripsi ini digunakan, sulit bagi penyadap untuk mematahkan *ciphertext*, sehingga komunikasi data antara pengirim dan penerima aman. Lebih lanjut mengenai enkripsi akan dijelaskan pada bagian selanjutnya. Pemonitoran terjadwal terhadap jaringan, proses memonitor dan melakukan administrasi terhadap keamanan jaringan akan dibahas pada bagian lain.

Dalam operasi jaringan, *availability* atau ketersediaan merupakan perhatian utama. Hal ini termasuk juga ketersediaan komponen perangkat keras, perangkat lunak, data, kapabilitas jaringan, dan sumber daya manusia. Pengendalian umum pada jaringan komputer adalah untuk memastikan hal berikut.

1. Lingkungan fisik yang memadai adalah sebuah kondisi di sekitar pengguna jaringan komputer yang mendukung semua kegiatan yang menggunakan jaringan komputer.
2. Ketersediaan sistem cadangan yang memadai jika terjadi masalah pada sistem jaringan utama termasuk di dalamnya suku cadang, perencanaan jika terjadi bencana, sistem *recovery* jaringan dan lain-lain.
3. Jaringan *peer to peer* merupakan salah satu cara untuk mengantisipasi jika jaringan utama tidak dapat dijalankan untuk dapat memungkinkan saling *backup*
4. Pelatihan dibutuhkan untuk mempersiapkan pengetahuan dari sumberdaya manusia dalam menghadapi kondisi jaringan yang mengalami masalah.

Kegiatan dan hal-hal yang membahayakan keamanan jaringan antara lain adalah hal-hal sebagai berikut.

1. *Probe* atau yang biasa disebut *probing* adalah suatu usaha untuk mengakses sistem atau mendapatkan informasi tentang sistem. Contoh sederhana dari *probing* adalah percobaan login ke suatu *account* yang tidak digunakan. *Probing* dapat dianalogikan dengan menguji kenop-kenop pintu untuk mencari pintu yang tidak dikunci sehingga dapat masuk dengan mudah. *Probing* tidak begitu berbahaya bagi sistem jaringan kita namun biasanya diikuti oleh tindakan lain yang lebih membahayakan keamanan.
2. *Scan* adalah *probing* dalam jumlah besar menggunakan suatu *tool*. *Scan* biasanya merupakan awal dari serangan langsung terhadap sistem yang oleh pelakunya ditemukan mudah diserang.
3. *Packet sniffer* adalah sebuah program yang menangkap (*capture*) data dari paket yang lewat di jaringan. Data tersebut bisa termasuk *user name*, *password*, dan informasi-informasi penting lainnya yang lewat di jaringan dalam bentuk text. Paket yang dapat ditangkap tidak hanya satu paket tapi bisa berjumlah ratusan bahkan ribuan, yang berarti pelaku mendapatkan ribuan *user name* dan *password*. Dengan *password* itu pelaku dapat mengirimkan serangan besar besaran ke sistem.
4. *Denial of Service*, *Denial of service* (DoS) bertujuan untuk mencegah pengguna mendapatkan layanan dari sistem. Serangan DoS dapat terjadi dalam banyak bentuk. Penyerang dapat membanjiri (*flood*) jaringan dengan data yang sangat besar atau dengan sengaja menghabiskan sumber daya yang memang terbatas, seperti *process control block* (PCB) atau *pending network connection*. Penyerang juga mungkin saja mengacaukan komponen fisik dari jaringan atau memanipulasi data yang sedang dikirim termasuk data yang terenkripsi.
5. *Social Engineering* / *Exploitation of Trust* sebuah cara untuk mempengaruhi orang dengan tujuan mengambil informasi penting dari orang atau perusahaan tertentu. Cara yang digunakan adalah dengan pendekatan sosial, teman, saudara

dan lainnya sehingga tercipta hubungan baik tapi tujuannya untuk mendapatkan informasi rahasia.

6. *Malicious Code Internet* adalah jenis kode komputer atau skrip *web* berbahaya yang dirancang untuk membuat kerentanan sistem yang mengarah ke *backdoor*, merusak keamanan sistem, pencurian informasi dan data, dan potensi kerusakan lainnya pada *file* dan sistem komputasi. Kejahatan ini biasanya tidak diblokir oleh sebagian perangkat lunak antivirus. Tidak semua perlindungan antivirus dapat menangani infeksi tertentu yang disebabkan oleh *malicious code*, yang berbeda dengan *malware*. *Malware* secara khusus mengacu pada perangkat lunak berbahaya, tetapi *malicious code* menyertakan skrip situs *web* yang dapat mengeksploitasi kerentanan untuk mengunggah perangkat lunak jahat.
7. *Infrastructure Attacks* adalah ancaman yang dapat merusak infrastruktur, ancaman yang paling sering terjadi adalah berupa serangan *denial of service* (DoS) yang membanjiri jaringan server atau *web server* dengan komunikasi palsu atau permintaan layanan palsu untuk merusak jaringan.

C. SISTEM MANAJEMEN BASIS DATA

Sistem manajemen basis data adalah struktur perangkat lunak atau perangkat keras yang mengendalikan sifat, dan akses ke informasi yang dibutuhkan oleh sistem aplikasi pengguna. Mengingat cara sistem dikembangkan selama bertahun-tahun, ada baiknya untuk memiliki pemahaman yang jelas tentang apa itu setiap komponen. Beberapa definisi atau istilah pada sistem manajemen basis data.

1. Metode akses: Prosedur logika perangkat lunak yang digunakan untuk mengambil, menyisipkan, memodifikasi, dan menghapus data pada perangkat penyimpanan.
2. Kamus data / sistem direktori data (DD / DS): Perangkat lunak yang mengelola tempat penyimpanan informasi tentang data dan lingkungan *database*.
3. Independensi data dan berbagi data: Independensi data adalah teknik yang memungkinkan beragam pengguna dengan pandangan logis berbeda untuk mengakses data yang sama dengan cara berbeda. Ini dicapai dengan memisahkan definisi sifat dan lokasi data dari program yang menggunakannya. Definisi, pandangan, aturan akses, lokasi, pandangan logis, dan informasi lain yang menjelaskan data sebenarnya terletak di satu *file* metadata, atau data tentang data. Hal ini memungkinkan pengguna baru dengan pandangan logis baru untuk diakomodasi serta mengubah pandangan logis dan mengubah representasi fisik.
4. Struktur data: Keterkaitan data dalam *database.*
5. *Database*: Kumpulan data yang diatur secara logis untuk memenuhi kebutuhan informasi dari semesta pengguna.
6. Administrasi basis data: Fungsi manusia yang terlibat dalam koordinasi dan pengendalian aktivitas terkait data.

7. *Database Management System* (DBMS): Sistem perangkat keras / perangkat lunak yang mengelola data dengan menyediakan fungsi organisasi, akses, dan kontrol.
8. Struktur penyimpanan: Metode dan teknik yang digunakan untuk merepresentasikan struktur data secara fisik pada perangkat penyimpanan.
9. Antarmuka sistem pengguna: Komponen lingkungan *database* yang meminta, memanipulasi, dan mengubah data menjadi informasi untuk pengguna akhir.

■ **Jenis Model *Database***

Ada banyak jenis model data. Beberapa yang paling umum termasuk di dalamnya adalah sebagai berikut.

a. Model *database* hirarkis (*Hierarchical database model*), model hierarkis mengatur data ke dalam struktur mirip pohon, di mana setiap catatan memiliki induk tunggal atau *root*. Dimana Catatan (*record*) dipilah dalam urutan tertentu dan perintah itu digunakan sebagai tatanan fisik untuk menyimpan *database*. Model ini bagus untuk menggambarkan banyak hubungan dunia nyata. Model ini digunakan pertama kali digunakan oleh sistem manajemen informasi IBM pada tahun 60-an dan 70-an, tetapi jarang digunakan pada saat ini karena faktor inefisiensi.
b. Model relasional (*Relational model*), model yang paling umum dimana model relasional mengurutkan data ke dalam tabel, juga dikenal sebagai relasi, yang masing-masing terdiri dari kolom dan baris. Setiap kolom mencantumkan atribut entitas yang dipermasalahkan, seperti harga, kode pos, atau tanggal lahir. Bersama-sama, atribut dalam relasi disebut domain. Atribut atau kombinasi atribut tertentu dipilih sebagai kunci utama yang dapat disebut di tabel lain, bila disebut kunci asing. Setiap baris, juga disebut *tupel*, mencakup data tentang *instance* spesifik entitas yang dimaksud, seperti karyawan tertentu. Model ini juga menjelaskan jenis hubungan antara tabel-tabel tersebut, termasuk hubungan satu ke satu, satu ke banyak, dan banyak ke banyak.
c. Model jaringan (*Network model*), model jaringan dibangun berdasarkan model hierarkis dengan memungkinkan banyak hubungan antara catatan terkait, yang menyiratkan banyak catatan orang tua (*parent records*). Berdasarkan teori himpunan matematis, model dibangun dengan serangkaian catatan terkait. Setiap set terdiri dari satu pemilik atau catatan induk dan satu atau lebih anggota atau catatan anak (*child records*). *Record* dapat menjadi anggota atau anak dalam beberapa set, memungkinkan model ini untuk menyampaikan hubungan yang kompleks. Model ini paling populer di tahun 70-an setelah secara formal didefinisikan oleh *Conference on Data Systems Languages* (CODASYL).
d. Model *database* berorientasi objek (*Object-oriented database model*) merupakan model yang mendefinisikan *database* sebagai kumpulan objek, atau elemen perangkat lunak yang dapat digunakan kembali, dengan fitur dan metode terkait.

Ada beberapa jenis *database* berorientasi objek: sebuah basis data multimedia menggabungkan media, seperti gambar, yang tidak bisa disimpan dalam *database* relasional. Sebuah basis data *hypertext* memungkinkan setiap objek untuk link ke objek lain. Ini berguna untuk mengatur banyak data yang berbeda, tetapi itu tidak ideal untuk analisis numerik. Model *database object-oriented* adalah model *database* pasca relasional yang paling dikenal, karena menggabungkan tabel, tetapi tidak terbatas pada tabel. Model semacam itu juga dikenal sebagai model basis data *hybrid.*

e. Model hubungan entitas (*Entity relationship model*), model ini menangkap hubungan antara entitas dunia nyata seperti model jaringan, namun tidak terkait langsung dengan struktur fisik *database*. Sering digunakan untuk merancang *database* secara konseptual. Di sini, orang-orang, tempat, dan hal-hal tentang titik-titik data yang disimpan disebut sebagai entitas, yang masing-masing memiliki atribut tertentu yang bersama-sama membentuk domain mereka. Kardinalitas, atau hubungan antar entitas, juga dipetakan.

f. Model relasional objek, model *database* hibrida ini menggabungkan kesederhanaan model relasional dengan beberapa fungsi lanjutan dari model *database* berorientasi objek. Pada intinya, ini memungkinkan desainer untuk menggabungkan objek ke dalam struktur tabel yang sudah dikenal. Bahasa dan antarmuka panggilan mencakup SQL3, bahasa vendor, ODBC, JDBC, dan antarmuka panggilan hak milik (*proprietary*) yang merupakan perpanjangan dari bahasa dan antarmuka yang digunakan oleh model relasional.

g. Model *file* terbalik (*Inverted file model*), *database* yang dibangun dengan struktur *file* terbalik dirancang untuk memudahkan pencarian teks secara cepat. Dalam model ini, konten data diindeks sebagai serangkaian kunci dalam tabel pencarian, dengan nilai yang menunjuk ke lokasi *file* yang terkait. Struktur ini dapat memberikan pelaporan data yang besar dan analitik secara cepat. Model ini telah digunakan oleh sistem manajemen *database* ADABAS dari *software* AG sejak tahun 1970, dan masih didukung sampai sekarang.

h. Model datar (*Flat model*), model datar adalah model data paling awal dan paling sederhana. Hanya mencantumkan semua data dalam satu tabel, terdiri dari kolom dan baris. Untuk mengakses atau memanipulasi data, komputer harus membaca seluruh *file* datar ke dalam memori, yang membuat model ini tidak efisien untuk semua kecuali set data terkecil.

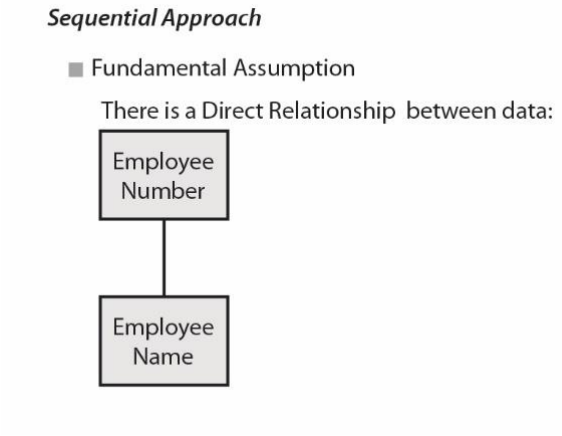
i. Model multidimensional (*Multidimensional model*), adalah variasi dari model relasional yang dirancang untuk memfasilitasi pemrosesan analitik yang lebih baik. Sedangkan model relasional dioptimalkan untuk pemrosesan transaksi *online* (*online transaction processing* = OLTP), model ini dirancang untuk pemrosesan analisis *online* (*online analytical processing* = OLAP). Setiap sel dalam basis data dimensi berisi data tentang dimensi yang dilacak oleh *database*. Secara visual, ini seperti sekumpulan kubus, bukan tabel dua dimensi.

j. Model semi struktur (*Semistructured model*). Dalam model ini, data struktural yang biasanya terdapat dalam skema *database* tertanam dengan data itu sendiri. Perbedaan antara data dan skema tidak jelas. Model ini berguna untuk menggambarkan sistem, seperti sumber data berbasis *web* tertentu, sebagai basis data tetapi tidak dapat dibatasi dengan skema. Berguna untuk menggambarkan interaksi antara *database* yang tidak mengikuti skema yang sama.

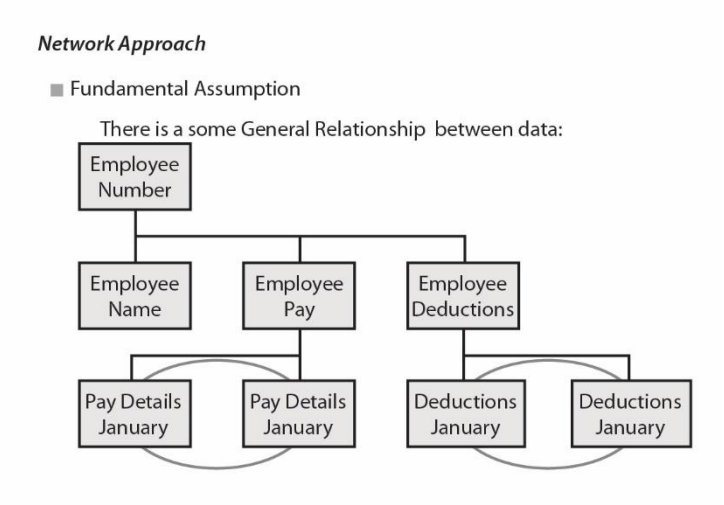
k. Model konteks (*Context model*). Model ini dapat menggabungkan elemen dari model *database* lain sesuai kebutuhan. Gabungan berbagai elemen dari model berorientasi objek, semistruktur, dan jaringan.

l. Model asosiatif (*Associative model*). Model ini membagi semua titik data berdasarkan apakah mereka menggambarkan entitas atau asosiasi. Dalam model ini, entitas adalah sesuatu yang ada secara independen, sedangkan asosiasi adalah sesuatu yang hanya ada dalam hubungannya dengan sesuatu yang lain. Model asosiatif struktur data menjadi dua set: Satu set item, masing-masing dengan pengidentifikasi unik, nama, dan tipe. Seperangkat tautan, masing-masing dengan pengidentifikasi unik dan pengenal unik dari sumber, kata kerja, dan target. Fakta yang tersimpan berkaitan dengan sumbernya, dan masing-masing dari ketiga pengidentifikasi dapat merujuk ke tautan atau item.

Di bawah ini ada tambahan penjelasan dari model *database* dalam bentuk gambar atau tabel.



Gambar 1.6
Sequential Approach



Gambar 1.7
Network Approach

Tabel 1.1
Relational Model

Relational Model

- *Fundamental Assumption*

There is some Mathatematical Relationship between data

Emp No	Dep No	NMW
12	15	F Bloffa
25	43	J Smith

Employee Table

Emp No	NMW
43	Internal Audit
47	IT

Depatemen Table

Data Manipulation

SELECT	— All Retrieval
UPDATE	— Change
INSERT	— Create new Tuple
DELETE	— Delete Tuple
FROM	— Specifies Table
WHERE	— Conditions
AND	— Conjunction of Conditions
OR	— Disjunction of Conditions

Example

SELECT	— EMPLOYEE = NAME FROM EMPLOYEE-DB WHERE
	— DEPT = “B03” AND POSITION = “MANAGER”

The result is always a table

Packages and Vendors

DB2	— IBM
DATACOM	— ADR

Inverted List

Record	**Make**	**Color**	**Model**
1	BMW	Red	528I
2	Ford	Blue	Laser
3	Ford	Red	Laser
4	BMW	Blue	328i

Can be indexed by Make, Color, Model

Make	***Record***
BMW	1,4
Ford	2,3
Color	***Record***

18	
Red	1,3
Ford	2,4
Model	***Records***
328I	5
528I	1
Laser	2,3

Kamus data / sistem direktori kamus data memberi tahu “apa” yang ada di dalam *database* / *file*. Ini berkaitan dengan deskripsi dari tampilan logis (yaitu, tampilan parsial dari data yang dimiliki pengguna dan termasuk item-item seperti, nama data, deskripsi, sinonim, dll.).

Direktori data memberi tahu “di mana dan bagaimana mengakses” data. Ini berkaitan dengan deskripsi aspek fisik data seperti, lokasi, alamat, dan representasi fisik. Entitas DD / DS ditentukan oleh atribut, yang mendeskripsikan data berikut ini.

a. Identifikasi
b. Sumber

c. Klasifikasi
c. Penggunaan
d. Kualifikasi
e. Hubungan

DD / DS dapat menjadi alat yang berguna terlepas dari kebutuhan DBMS di bidang dukungan dokumentasi, koordinasi penggunaan data bersama, dan kontrol atas modifikasi program dan *file*. DD / DS telah menjadi populer dengan munculnya paket DBMS dengan pengenalan yang lebih besar atas peluang untuk berbagi data, yang mengarah pada kebutuhan yang lebih besar untuk mengontrol penggunaan data, pengenalan undang-undang privasi komputer di masa mendatang, serta kompleksitas hubungan yang terlibat.

Siapa yang merawat sistem *database*? Administrator basis data. Fungsi DBA termasuk mengkoordinasikan konten informasi dari *database*. Ini tidak berarti bahwa data aktual itu sendiri menjadi perhatian DBA, tetapi DBA bertanggung jawab untuk memutuskan struktur penyimpanan dan strategi akses. DBA akan bekerja sama dengan pengguna komputer dan, mengikuti persyaratan bisnis mereka, akan menetapkan pemeriksaan otorisasi dan prosedur validasi serta strategi untuk pencadangan dan pemulihan. DBA juga bertanggung jawab untuk memantau kinerja dan menanggapi perubahan persyaratan.

Untuk mencapai semua tujuan ini, DBA memiliki alat pembuangan yang dirancang khusus untuk memfasilitasi tugas-tugas ini. Alat-alat ini termasuk program utilitas untuk mengizinkan pemuatan data mentah ke *database*, rutinitas reorganisasi untuk menjaga akses *database* tetap efisien dan efektif, dan analisis statistik untuk menentukan kapan pemeliharaan diperlukan. Selain itu, penjurnalan (misalnya, log) dapat menyimpan catatan tentang siapa yang melakukan apa dan kapan di *database*. Meskipun log ini bersifat opsional, log ini dapat menjadi bantuan utama untuk DBA dalam pemulihan *database* jika terjadi masalah. Kamus Data itu sendiri, selain penganalisis *database*, juga akan membantu dalam pemulihan.

Pemulihan basis data, tujuan dari pemulihan basis data adalah untuk memulihkan basis data ke keadaan yang diketahui sambil meminimalkan pekerjaan yang hilang. Ini berarti bahwa ia harus mengizinkan pemulihan atas dasar transaksi dan menyediakan pemulihan cepat untuk meminimalkan pekerjaan manual sekaligus memastikan keamanan data pemulihan. Pada saat yang sama, tidak dapat dihindari dalam proses seperti itu bahwa beberapa data pada akhirnya akan hilang dan pemulihan harus menyediakan mekanisme untuk menginformasikan pengguna tentang transaksi yang “hilang”. Pemulihan harus memenuhi berbagai jenis kegagalan termasuk bencana perangkat keras dan perangkat lunak.

Prosedur pemulihan datang dalam berbagai bentuk untuk menangani berbagai bentuk kegagalan dan meliputi:

a. Pos pemeriksaan. DBMS akan menentukan atau memaksakan suatu titik waktu di mana semua transaksi telah dilakukan, dimasukkan ke disk, dan semua buffer memori telah dihapus. Pada titik ini, sebuah catatan dibuat bahwa *database* "diam" atau telah "di-*quiessed*" dan bahwa pemulihan apa pun hanya perlu kembali sejauh ini. Ini digunakan untuk menentukan status "stabil" dari *database* untuk pemulihan.
b. *Roll Back*. Log diproses mundur dan transaksi yang diselesaikan diluncurkan ke pos pemeriksaan terakhir.
c. *Roll Forward*. Log diproses ke depan untuk memulihkan sistem.
d. Perbarui salinan cadangan. (mis., kegagalan media)
e. Transaksi kompensasi. (misalnya, entri jurnal)
f. Rutinitas keselamatan.

Untuk pemulihan log yang efektif, sebelum *database* diperbarui, log dari gambar sebelumnya dibuat untuk mengaktifkan pembatalan perubahan jika perlu (misalnya, kegagalan sebelum pembaruan). Setelah *database* diperbarui, log gambar setelah dibuat untuk mengulangi perubahan jika perlu (misalnya, kegagalan media). Log ini berisi informasi jejak audit untuk tindak lanjut manual (misalnya, id program, id transaksi).

D. PROSES AUDIT SISTEM INFORMASI TERKAIT DENGAN *DATABASE*

Dengan munculnya DBMS, ini telah menjadi migrasi kontrol dari aplikasi individu ke lingkungan *database* umum. Migrasi kontrol ini meningkatkan peluang kontrol secara keseluruhan dan memungkinkan administrasi terpusat dari lingkungan kontrol. Untuk meninjau desain *database* yang relevan, proses audit sistem informasi akan:

1. Buat daftar semua jenis *record*. Kegiatan ini bertujuan untuk menelusuri setiap transaksi yang tersimpan dalam *database* untuk memudahkan *tracking record* data dalam sistem
2. Membaca dan menganalisis deskripsi dan nama data. Tujuan kegiatan ini adalah untuk memahami data dan hubungan antar data dalam sistem
3. Identifikasi kunci dari setiap *record* dan verifikasi persyaratannya. Tujuan dari kegiatan ini adalah untuk memeriksa atau verifikasi dari setiap *record* yang tersimpan
4. Keunikan data dan mempelajari hubungan antar data. Tujuan dari kegiatan ini adalah memastikan *database* yang dirancang sesuai dengan aturan pembuatan *database* secara umum misalnya adanya kode unik untuk setiap tabel, hubungan kardinalitas yang benar antar tabel atau objek seperti *one to many*, *one to one* atau *many to many*, identifikasi semua hubungan.

5. Verifikasi konsistensi desain dengan kebutuhan informasi bisnis merupakan tahapan akhir data proses audit terkait dengan struktur *database* untuk melihat rancangan *database* dengan proses bisnis.

Proses audit sistem informasi terkait dengan *database* dapat menggunakan dokumentasi atau kamus data / direktori data dimana dokumen ini dapat digunakan untuk menerima, merekam, dan menghasilkan berbagai dokumentasi, termasuk:

1. persyaratan dan spesifikasi,
2. dokumentasi data,
3. pembuatan metadata.

Proses ini dapat mengotomatiskan proses dokumentasi dan memungkinkan referensi silang program ke elemen data individu serta pembuatan laporan. Ini juga dapat membantu dalam menegakkan kontrol perubahan. Kamus data dapat dibangun dengan pendekatan yaitu mode aktif atau pasif. Dalam mode aktif, semua akses *database* harus dilakukan melalui DD / DS. Dalam mode pasif DD / DS ada di sana sebagai catatan, tetapi memiliki kontrol efektif yang sangat sedikit. Keuntungan nyata dari *active* DD / DS termasuk peningkatan akurasi, ketepatan waktu, kelengkapan, dan kontrol.

Adapun proses audit sistem informasi adalah sebagai berikut.

1. **Fungsi administrasi dan koordinasi auditor**, Fungsi administrasi dan koordinasi dengan memeriksa kegiatan tinjauan dan pemantauan DBA, yang akan mencakup tinjauan desain basis data, tinjauan desain sistem, tinjauan desain program, dan pengkodean, pemantauan kualitas umum data, dan memantau kinerja *database* secara keseluruhan. Masalah organisasi seperti peran yang memerlukan segregasi juga akan diperiksa. Ini biasanya mencakup:
   a. administrasi basis data,
   b. pengembangan sistem,
   c. pemrograman,
   d. operasi,
   e. pengguna akhir,
   f. audit internal.

   Ini hanya dapat dilakukan secara efektif dengan memberikan tanggung jawab atas kepemilikan data. Hal ini dapat mengurangi kekhawatiran pengendalian pembagian tanggung jawab pembaruan data yang tidak terkoordinasi dengan menetapkan tanggung jawab definisi. Koordinasi penggunaan bersama seperti itu memastikan penerapan seragam dari tingkat kontrol yang sesuai.
2. **Pengendalian operasional untuk lingkungan basis data**. Dalam pengoperasian sistem bisnis terstruktur basis data, auditor harus memastikan keberadaan dan efektivitas pengendalian untuk memastikan akses yang tidak sah, kontrol untuk memastikan akurasi dan kelengkapan, alat dan teknik Pemulihan dan *Restart*, dan

kontrol atas akses ke data. Dampak lingkungan *database* pada privasi dan keamanan diperumit oleh kebutuhan untuk menilai persyaratan di antara banyak pengguna. Berbagi data dapat menyebabkan masalah kontrol; namun, dimungkinkan untuk mendeskripsikan spesifikasi keamanan menggunakan *Declarative Data Definition Language* (DDL), sehingga secara terpusat memastikan spesifikasi yang lebih jelas dan membuat lingkungan lebih mudah untuk diaudit. Hal ini disebabkan oleh migrasi implementasi kontrol dari aplikasi ke lingkungan.

3. **Dampak *database* pada masalah kelengkapan dan keakuratan**. Teknologi *database* dapat memiliki pengaruh yang nyata pada kualitas informasi yang diberikan. Ini adalah konsentrasi risiko karena berbagi data dan peningkatan biaya koreksi kesalahan karena kompleksitas sistem. Selain itu, mungkin ada efek yang memburuk pada kepercayaan dan kepercayaan pengguna karena erosi *database* dan kesalahan berjenjang. Mengurangi kekhawatiran yang melibatkan kelengkapan dan keakuratan berarti bahwa tidak hanya risiko tetapi juga kontrol harus berpindah. Ini dapat digeneralisasikan di lingkungan dan diimplementasikan di DBMS, DD / DS, dan seterusnya. Manfaat dari sudut pandang auditor termasuk potensi untuk:
   a. konsistensi data, dengan tersedianya *database* yang terstruktur akan memudahkan proses audit karena semuanya sudah terdokumentasi;
   b. meningkatkan kualitas audit dengan meningkatkan aksesibilitas, dengan tersedianya *database* yang terstruktur akan meningkatkan hasil dari penilaian sistem informasi khususnya *database;*
   c. proses pengembangan sistem yang lebih akurat, *database* yang terstruktur juga memudahkan inisiasi untuk pengembangan sistem kedepan.

   Sedangkan kerugian dari sudut pandang auditor meliputi berikut ini.
   a. Sindrom teknologi, diperlukan pengetahuan yang cukup dalam untuk memahami domain *database* beserta teknologi yang mendukung berdampak pada kekhawatiran untuk melakukan proses audit karena keterbatasan pengetahuan yang dimiliki.
   b. Pengendalian biaya implementasi, anggaran merupakan hal yang sensitif dalam konteks pemeriksaan yang menyeluruh karena diperlukan upaya yang lebih besar sehingga membutuhkan anggaran tambahan.
   c. Akses ke data yang dikelola DBMS, pembatasan akses terkadang menjadi kendala khusus dalam proses audit sistem informasi. pembatasan tersebut disebabkan banyak alasan tapi pada akhirnya akan menghambat proses audit.
   d. Perubahan integritas data, perubahan pada struktur *database* yang tidak terdokumentasi akan menyulitkan proses audit. Kalaupun sudah

didokumentasikan dengan baik tetap membutuhkan upaya yang lebih besar untuk memahami perubahan yang terjadi.

e. Perubahan ruang lingkup / waktu audit, perubahan ruang lingkup menjadi masalah yang sering terjadi ketika saat proses audit berjalan ditemukan hal yang saling berkaitan antara satu bagian dengan bagian lainnya sehingga secara tidak langsung memperluas lingkup dan waktu pelaksanaan audit.

Upaya auditor dalam lingkungan yang berubah seperti itu adalah

a. berkonsultasi dengan pengguna *database* tentang persyaratan untuk proses pemeriksaan;
b. memeriksa aturan edit dan validasi dari proses audit;
c. menentukan apakah ada toleransi atas kesepakatan yang telah di tentukan pada awal perjanjian;
d. berkonsultasi terhadap orang yang bertanggung jawab terhadap bagian *database*.

Kualitas yang membantu auditor dalam tugas ini meliputi kemampuan untuk mengedit dan validasi elemen demi elemen, *error response*, prosedur edit dan pemeliharaan validasi, dan prosedur untuk menambahkan elemen data baru.

Studi kasus: Laptop yang dicuri

Komputer laptop baru dikeluarkan untuk digunakan oleh beberapa anggota staf terpilih di departemen dalam organisasi besar. Laptop disimpan dalam lemari arsip *overhead* yang terkunci di lantai yang tidak aman di gedung kantor utama organisasi. Kunci lemari disimpan dalam cangkir di meja pengguna utama, dan penutup ditempatkan di atas cangkir. Suatu hari, sekitar seminggu setelah laptop dikirimkan, laptop itu dicuri dari lemari penyimpanan di atas kepala yang terkunci.

Departemen audit internal diberitahu tentang situasi tersebut dan melakukan penyelidikan. Dua orang yang bekerja dengan laptop tersebut adalah administrator keamanan jaringan area lokal (LAN) dari departemen dan spesialis komputer mikro dari departemen layanan jaringan. Keduanya telah bekerja di organisasi selama kurang dari tiga bulan. Riwayat pekerjaan dan pemeriksaan latar belakang polisi dari kedua individu tersebut diperiksa untuk menentukan apakah profil mereka dapat mengidentifikasi mereka sebagai kandidat untuk pencurian laptop. Juga, karyawan yang dimaksud diwawancarai. Namun, tanpa bukti “kuat”, tidak mungkin untuk menentukan apakah laptop dicuri oleh salah satu dari dua karyawan pengguna utama, beberapa karyawan lain di gedung, pelanggan yang ada di gedung, vendor, atau penjaga. Organisasi tidak mengalami kerugian finansial langsung karena laptop telah diasuransikan. Namun, banyak waktu staf dihabiskan untuk mengkonfigurasi ulang laptop baru, dan peningkatan produktivitas yang diharapkan di departemen pengguna tertunda selama beberapa minggu.

Akibat pencurian ini, semua laptop di organisasi dilengkapi dengan perangkat pengunci kabel. Moral dari cerita ini: Jangan mengandalkan penguncian lemari penyimpanan di atas kepala, lemari arsip, atau lemari untuk keamanan peralatan komputer yang mahal kecuali kunci dan suku cadang telah diamankan dengan benar.

Sisi positifnya, pencurian laptop ini mengakibatkan pemulihan. Selama pencarian laptop yang hilang, laptop departemen audit internal yang telah hilang selama beberapa minggu ditemukan. Untungnya, auditor secara tidak sengaja meninggalkannya di gudang kantor utama, dan sedang "disimpan" oleh manajer gudang karena dia tidak tahu milik siapa laptop tersebut.

Arson dan vandalisme adalah kejahatan lain yang sering terlihat yang dapat mengakibatkan kerusakan pada sumber daya komputer organisasi. Tidak seperti ibu pertiwi, beberapa bahaya manusia yang merusak mungkin tidak selalu terlihat. Misalnya, lonjakan daya listrik dapat secara instan membakar sirkuit komputer dan periferal, dan gangguan yang berbahaya dapat mengakibatkan kerusakan internal pada perangkat keras komputer serta data yang hilang, rusak, atau terganggu.

Tidak ada bagian dunia yang kebal terhadap bahaya alam dan manusia. Oleh karena itu, semua organisasi harus memiliki kontrol internal yang membantu mengurangi dampak bencana ini pada operasi yang berkelanjutan. Namun, kontrol keamanan fisik dalam banyak organisasi sangat tidak memadai. Ini adalah peran semua auditor, termasuk mereka yang bertugas memeriksa sistem informasi, untuk mengidentifikasi kelemahan kontrol keamanan fisik yang signifikan dan untuk menyampaikan rekomendasi kepada manajemen untuk mengatasi kelemahan ini.

Salah satu pengendalian preventif yang paling jelas, tetapi sering diabaikan adalah menempatkan peralatan komputer utama di suatu tempat di atas lantai pertama fasilitas. Beberapa waktu yang lalu, sebuah pusat data untuk perusahaan asuransi besar di Midwest memasang peralatan komputernya di ruang bawah tanah sebuah gedung perkantoran. Selama banjir yang tidak terduga, ruang bawah tanah dengan cepat terisi air dan peralatan menjadi tidak berguna. (Untungnya, perusahaan memiliki prosedur memulai kembali bisnis yang memadai untuk meminimalkan gangguan layanan). Dalam kasus ini, karena parahnya banjir, peralatan komputer akan rusak parah meskipun terletak di lantai pertama. Namun, seandainya peralatan dipasang di lantai dua atau lebih tinggi, tidak akan ada kerusakan sama sekali. Memang, layanan akan tetap terganggu karena catu daya, kabel listrik, dan peralatan telekomunikasi tidak berfungsi, tetapi peralatan itu sendiri tidak perlu diperbaiki atau diganti.

Selain lokasi, sejumlah jenis kunci kontrol keamanan fisik harus diterapkan dalam organisasi, termasuk berikut ini.

1. Berbagai jenis kunci fisik, termasuk kunci tombol konvensional, kunci lencana akses elektronik, kunci sandi, kunci kombinasi, dan kunci biometrik.
2. Petugas keamanan.
3. Kamera pengintai video.
4. Prosedur darurat dan deteksi umum.

5. Sistem pemanas, ventilasi, dan pendingin (HVAC).
6. Perlindungan asuransi atas perangkat keras dan biaya untuk membuat ulang data.
7. Prosedur untuk melakukan pencadangan perangkat lunak sistem, program aplikasi, dan data secara berkala serta penyimpanan dan rotasi media cadangan ke lokasi di luar situs yang aman.
8. Daya darurat dan sistem catu daya tak terputus (UPS).

Latihan

Untuk memperdalam pemahaman Anda mengenai materi di atas, kerjakanlah latihan berikut!

1) Jelaskan perbedaan sistem pengendalian dari sistem berbasis manual dengan sistem berbasis komputer!
3) Jelaskan aktivitas audit sistem informasi terkait dengan *database* dan perangkat keras!
4) Jelaskan hubungan desain *database* dengan audit sistem informasi!

Petunjuk Jawaban Latihan

1) Secara substansial perbedaan keduanya adalah otomatisasi kontrol yang berdampak signifikan terhadap sistem.
2) Aktivitas audit sistem informasi dalam konteks *database* dan perangkat keras adalah bagaimana pengadaan dan penggunaan *database* dapat dimonitor dan dikendalikan untuk keamanan sistem informasi.
3) Rancangan *database* yang standar akan memudahkan proses audit sistem informasi karena *database* merupakan bagian penting dari sistem sebagai media penyimpanan.

Rangkuman

1. Beberapa Istilah Komputasi: CPU *(Central Processing Unit)*, Terminal komputer, printer, perangkat penyimpanan mobile seperti *flash disk*, *harddisk* eksternal, memori. Perangkat lunak, memori, modem, *multiplexer*, serat optik, *microwave*, *keyboard*, *mouse*, pemindai, *barcode*, QR Code atau *quick respons code*, RFID dan *voice recognition*.
2. Beberapa jenis jaringan berdasarkan luas jangkauan : LAN atau *local area network*, MAN atau *metropolitan area network* dan WAN atau *wide area network System.* keamanan jaringan adalah untuk menentukan data atau informasi apa saja yang harus dilindungi, menentukan berapa besar biaya yang harus ditanamkan

dalam melindunginya dan menentukan siapa yang bertanggung jawab untuk menjalankan langkah-langkah yang diperlukan untuk melindungi bagian tersebut.

3. Pembatasan akses pada suatu jaringan beberapa konsep yang ada dalam pembatasan akses jaringan, yaitu *Internal Password Authentication*., *Server-based password authentication* dan *Firewall* dan *Routing Control*.
4. Pengendalian umum pada jaringan komputer adalah untuk memastikan lingkungan fisik yang memadai, ketersediaan sistem cadangan yang memadai, jaringan *peer to peer* dan pelatihan.
5. Untuk meninjau desain *database* yang relevan, proses audit sistem informasi dilakukan dengan membuat daftar semua jenis *record*, membaca dan menganalisis deskripsi dan nama data, identifikasi kunci dari setiap *record* dan verifikasi persyaratan dan keunikan data dan mempelajari hubungan antar data.
6. Ada banyak jenis model data. Beberapa yang paling umum termasuk di dalamnya adalah model *database* hirarkis (*Hierarchical database model*), model relasional (*Relational model*), model jaringan (*Network model*), model *database* berorientasi objek (*Object-oriented database model*) , model hubungan entitas (*Entity relationship model*) dan model *file* terbalik (*Inverted file model*).

Tes Formatif 2

Pilihlah satu jawaban yang paling tepat!

1) Berikut ini adalah tahapan yang harus dilakukan untuk melindungi keamanan data yang berhubungan dengan perangkat keras, *kecuali* ....
   A. perencanaan, yaitu kegiatan membuat rencana semua kegiatan yang dilakukan selama kegiatan audit sistem informasi
   B. *acquisistion* adalah kegiatan menganalisis sumber perangkat keras yang digunakan oleh perusahaan untuk mendukung sistem informasi yang digunakan oleh perusahaan
   C. *implementation* adalah kegiatan memahami dan mengawasi instalasi perangkat keras yang digunakan untuk mendukung sistem informasi perusahaan
   D. evaluasi adalah kegiatan memahami proses pemeliharaan perangkat keras yang digunakan untuk mendukung sistem informasi perusahaan

2) Suatu model pengolahan data, dengan menghimpun data terlebih dahulu, dan diatur pengelompokan datanya dalam kelompok-kelompok yang disebut ....
   A. *batch processing*
   B. *online processing*
   C. *real time processing*
   D. *offline processing*

3) Adalah orang yang ditunjuk dalam sebuah organisasi yang tanggung jawabnya mencakup pemeliharaan infrastruktur komputer dengan penekanan pada jaringan ....
   A. *database administrator*
   B. *network administrator*
   C. *sistem administrator*
   D. *office administrator*

4) Adalah proses yang menyandikan pesan atau *file* sehingga hanya bisa dibaca oleh orang-orang tertentu ....
   A. deskripsi
   B. konkurensi
   C. enkripsi
   D. akurasi

5) Komunikasi daring sinkron (serempak) yaitu komunikasi *online* yang dilakukan secara bersamaan dan menggunakan media komputer untuk komunikasi dengan konsep waktu *realtime* ....
   A. *Enkripsi*
   B. *Duplex*
   C. *Asinkron*
   D. *Sinkron*

6) Adalah sistem yang mengelola unit pemrosesan pusat atau CPU yang terhubung ke berbagai perangkat *periferal* yang membantu dalam menyimpan, mengakses, dan mengirimkan data dan juga dalam produksi keluaran informasi sistem ....
   A. operasi
   B. pendukung
   C. aplikasi
   D. komputer

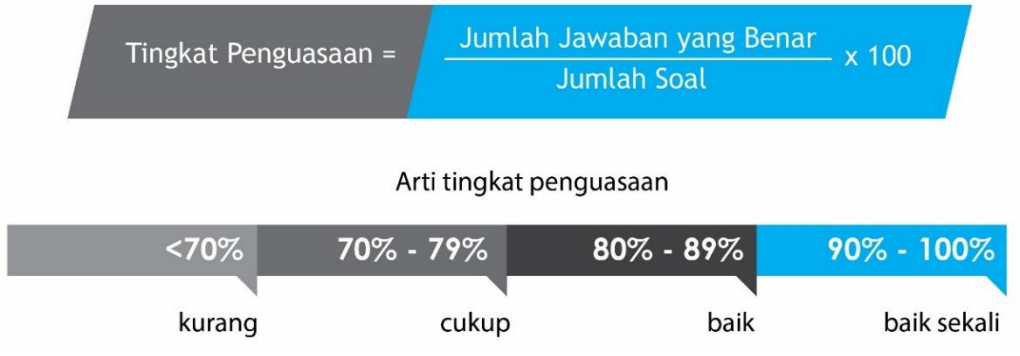
7) Masalah baru yang berakibat dari keterbukaan akses internet adalah, *kecuali* ....
   A. pemeliharaan validitas dan integritas data atau informasi tersebut
   B. jaminan ketersediaan informasi bagi pengguna yang berhak
   C. pencegahan akses sistem dari yang tidak berhak
   D. sistem *offline*

8) Sebuah cara untuk mempengaruhi orang dengan tujuan mengambil informasi penting dari orang atau perusahaan tertentu. Cara yang digunakan adalah dengan pendekatan sosial seperti teman, saudara dan lainnya sehingga tercipta hubungan baik tapi tujuannya untuk mendapatkan informasi rahasia ....
   A. *social engineering / exploitation of trust*
   B. sosial media
   C. *social commerce*
   D. *social learning*

9) Model *database* yang mengatur data ke dalam struktur mirip pohon, di mana setiap catatan memiliki induk tunggal atau *root*. Dimana catatan (*record*) dipilah dalam urutan tertentu dan perintah itu digunakan sebagai tatanan fisik untuk menyimpan *database*. Model ini bagus untuk menggambarkan banyak hubungan dunia nyata, model ....
   A. *database* hirarkis
   B. terstruktur
   C. *online*
   D. sistematis

10) Kegiatan audit sistem informasi terkait dengan *database* adalah, *kecuali* ....
   A. buat daftar semua jenis *record*
   B. membaca dan menganalisis deskripsi dan nama data
   C. identifikasi kunci dari setiap *record* dan verifikasi persyaratannya
   D. melakukan evaluasi

Cocokkanlah jawaban Anda dengan Kunci Jawaban Tes Formatif 2 yang terdapat di bagian akhir modul ini. Hitunglah jawaban yang benar. Kemudian, gunakan rumus berikut untuk mengetahui tingkat penguasaan Anda terhadap materi Kegiatan Belajar 2.



Apabila mencapai tingkat penguasaan 80% atau lebih, Anda dapat meneruskan dengan modul selanjutnya. **Bagus!** Jika masih di bawah 80%, Anda harus mengulangi materi Kegiatan Belajar 2, terutama bagian yang belum dikuasai.

Kunci Jawaban Tes Formatif

Tes Formatif 1

1) A
2) A
3) C
4) D
5) D
6) A
7) A
8) B
9) B
10) A

Tes Formatif 2

1) D
2) A
3) B
4) C
5) D
6) A
7) D
8) A
9) A
10) D

Glosarium

Computer systems engineer	:	Jabatan yang bertanggung jawab untuk mengidentifikasi solusi untuk masalah aplikasi yang kompleks, masalah administrasi sistem, atau masalah jaringan.
Denial of service (DoS)	:	Bertujuan untuk mencegah pengguna mendapatkan layanan dari sistem. Serangan DoS dapat terjadi dalam banyak bentuk. Penyerang dapat membanjiri (*flood*) jaringan dengan data yang sangat besar atau dengan sengaja menghabiskan sumber daya yang memang terbatas, seperti *process control block* (PCB) atau *pending network connection.*
Entity relationship model	:	Model ini menangkap hubungan antara entitas dunia nyata seperti model jaringan, namun tidak terkait langsung dengan struktur fisik *database*. Sering digunakan untuk merancang *database* secara konseptual
Infrastructure Attacks	:	Ancaman yang dapat merusak infrastruktur, ancaman yang paling sering terjadi adalah berupa serangan *denial of service* (DoS) Membanjiri jaringan server atau web server dengan komunikasi palsu atau permintaan layanan palsu untuk merusak jaringan.
Kontrol keamanan fisik	:	Kontrol terhadap semua perangkat keras komputer termasuk CPU dan semua perangkat periferal termasuk jaringan dan telekomunikasi.
Kontrol keamanan logis	:	Perlindungan keamanan atas sistem komputasi secara memadai dari akses yang tidak sah dan kerusakan yang tidak disengaja atau disengaja atau perubahan program perangkat lunak sistem.
Malicious Code Internet	:	Jenis kode komputer atau skrip *web* berbahaya yang dirancang untuk membuat kerentanan sistem yang mengarah ke *backdoor*, merusak keamanan sistem, pencurian informasi dan data, dan potensi kerusakan lainnya pada *file* dan sistem komputasi.

Model *file* terbalik *(Inverted file model)*	:	Model *database* yang dibangun dengan struktur *file* terbalik dirancang untuk memudahkan pencarian teks secara cepat. Dalam model ini, konten data di indeks sebagai serangkaian kunci dalam tabel pencarian, dengan nilai yang menunjuk ke lokasi *file* yang terkait.
Packet Sniffer	:	Sebuah program yang menangkap (*capture*) data dari paket yang lewat di jaringan. Data tersebut bisa termasuk *user* name, *password*, dan informasi-informasi penting lainnya yang lewat di jaringan dalam bentuk text. Paket yang dapat ditangkap tidak hanya satu paket tapi bisa berjumlah ratusan bahkan ribuan, yang berarti pelaku mendapatkan ribuan *user name* dan *password*. Dengan *password* itu pelaku dapat mengirimkan serangan besar besaran ke sistem.
Pengendalian khusus sistem informasi	:	Pengendalian aplikasi baik manual dan terkomputerisasi, dalam aplikasi bisnis untuk memastikan data tersebut diproses secara lengkap, akurat, dan tepat waktu.
Pengendalian umum sistem informasi	:	Pengendalian yang mengatur lingkungan dimana sistem informasi dibangun, dikembangkan, dipelihara, dan dioperasikan. Pengendalian yang mencakup standar pembangunan dan pengembangan sistem yang dioperasikan oleh organisasi, pengendalian yang berlaku untuk pengoperasian instalasi komputer termasuk didalamnya perangkat keras, perangkat lunak, teknologi jaringan dan semua bagian yang berhubungan dengan sistem berbasis komputer.
RFID	:	*Radio Frequency Identification* adalah teknologi yang menggunakan gelombang radio untuk secara pasif mengidentifikasi objek yang diberi tag. Teknologi ini digunakan dalam beberapa aplikasi komersial dan industri, untuk melacak item di sepanjang rantai pasokan untuk melacak item yang diperiksa dari perpustakaan.

Daftar Pustaka

Cascarino, R. E. (2007). *Auditor's guide to information systems auditing*. John Wiley & Sons.

Champlain, J. J. (2003). *Auditing information systems*. John Wiley & Sons.

Hall, J. A. (2015). *Information technology auditing*. Cengage Learning.