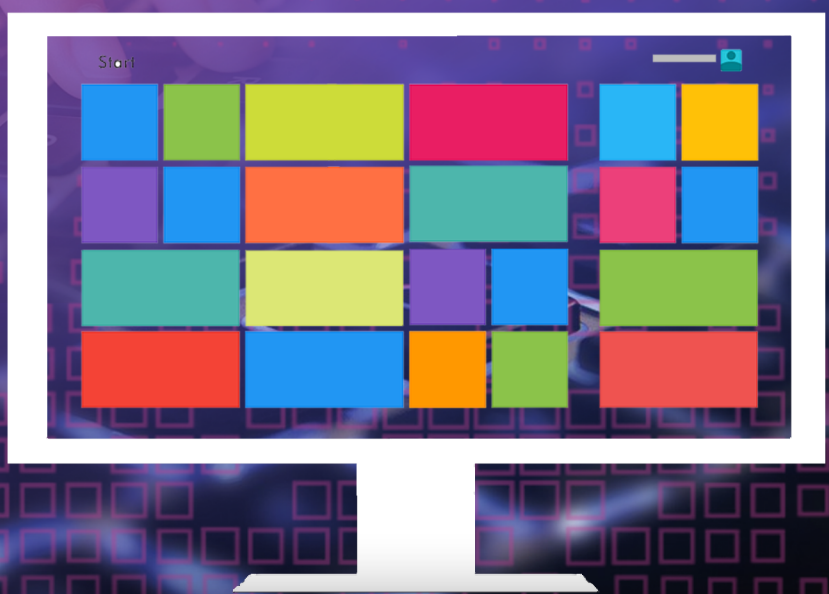
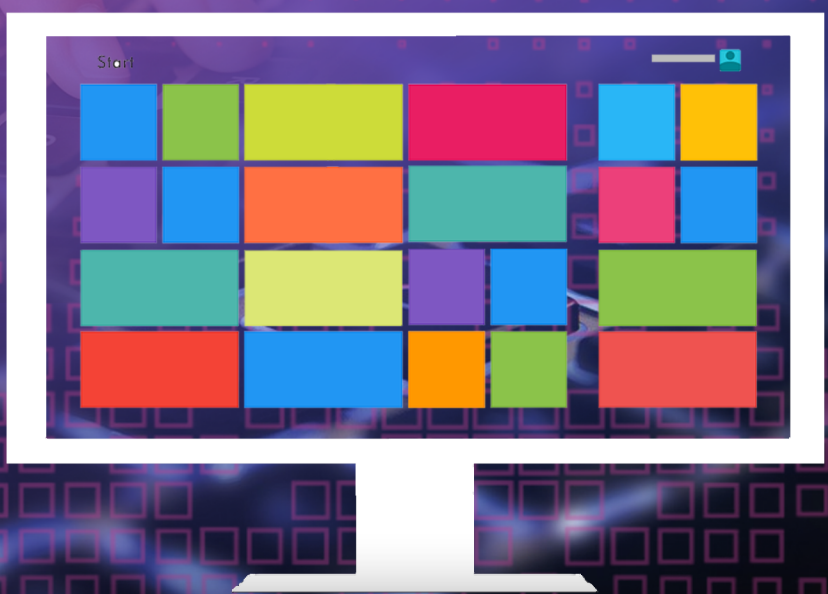
Audit Sistem Informasi



Silvia Ratna

Audit Sistem Informasi



UU 28 tahun 2014 tentang Hak Cipta

Fungsi dan sifat hak cipta Pasal 4

Hak Cipta sebagaimana dimaksud dalam Pasal 3 huruf a merupakan hak eksklusif yang terdiri atas hak moral dan hak ekonomi.

Pembatasan Perlindungan Pasal 26

Ketentuan sebagaimana dimaksud dalam Pasal 23, Pasal 24, dan Pasal 25 tidak berlaku terhadap:

a. penggunaan kutipan singkat Ciptaan dan/atau produk Hak Terkait untuk pelaporan peristiwa aktual yang ditujukan hanya untuk keperluan penyediaan informasi aktual;
b. Penggandaan Ciptaan dan/atau produk Hak Terkait hanya untuk kepentingan penelitian ilmu pengetahuan;
c. Penggandaan Ciptaan dan/atau produk Hak Terkait hanya untuk keperluan pengajaran, kecuali pertunjukan dan Fonogram yang telah dilakukan Pengumuman sebagai bahan ajar; dan
d. penggunaan untuk kepentingan pendidikan dan pengembangan ilmu pengetahuan yang memungkinkan suatu Ciptaan dan/atau produk Hak Terkait dapat digunakan tanpa izin Pelaku Pertunjukan, Produser Fonogram, atau Lembaga Penyiaran.

Sanksi Pelanggaran Pasal 113

1. Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf c, huruf d, huruf f, dan/atau huruf h untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan/atau pidana denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah).
2. Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf a, huruf b, huruf e, dan/atau huruf g untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

Audit Sistem Informasi

Silvia Ratna

Penerbit Yayasan Kita Menulis

Audit Sistem Informasi

Penulis:
Silvia Ratna

Editor: Suginam & Endra Saputra
Desain Sampul: Devy Dian Pratama, S.Kom.

Penerbit
Yayasan Kita Menulis
Web: kitamenulis.id
e-mail: press@kitamenulis.id
WA: 0821-6453-7176
IKAPI: 044/SUT/2021

Silvia Ratna
Audit Sistem Informasi
Yayasan Kita Menulis, 2023
viii; 70 hlm; 16 x 23 cm
ISBN: 978-623-342-860-6
Cetakan 1, Juni 2023
I. Audit Sistem Informasi
II. Yayasan Kita Menulis

Katalog Dalam Terbitan

Kata Pengantar

Puji syukur kami panjatkan kehadirat Allah SWT karena dengan rahmat, karunia, serta taufik dan hidayah-Nya kami dapat menyelesaikan Buku tentang "Audit Sistem Informasi" ini dengan baik meskipun banyak kekurangan didalamnya. Kami berharap agar kiranya buku ini dapat digunakan dengan sebaik baikanya bagi kalangan mahasiswa, dosen dan penggunal lainya.

Adapaun Pokok Bahasan dari Buku ini Pengenalan Audit Sistem Informasi, Kontor; Audit Sistem Informasi, Pendekatan Audit Sistem Informasi, Sistem Pengendali Audit Sistem Informasi, Sistem berbasis Teknologi Informasi

Saya berharap jika ada yang salah mohon kiranya diberika masukan yang sifatnya membangun. Dan menjadikan lebih baik kedepanya.

Banjarmasin, Juni 2023

Penulis

Daftar Isi

Bab 4 Sistem Pengendali Audit Sistem Informasi

Bab 5 Sistem Berbasis Teknologi Informasi

Bab 1

Apa Itu Audit Sistem Informasi?

1.1 Pendahuluan

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 di mana 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.

1.2 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 instalasikomputer termasuk di dalamnya 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 inputnya. 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 di mana 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.

1.3 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. Di mana 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, di mana 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 di mana 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) di mana 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.

1.4 Konsep Komunikasi Audit Sistem Informasi

Penggunaan jenis sarana komunikasi akan memengaruhi 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 di mana 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.

Bab 2

Kotrol Audit Sistem Informasi

2.1 Pendahuluan

Kontrol adalah sebuah sistem untuk mencegah, mendeteksi atau memperbaiki situasi yang tidak teratur. Terdapat tiga aspek penting yang berkaitan dengan definisi kontrol di atas, yaitu:

1. Kontrol adalah sebuah sistem, dengan kata lain kontrol terdiri atas sekumpulan komponen-komponen yang saling berhubungan dan bekerja sama untuk mencapai tujuan yang sama.
2. Fokus dari kontrol adalah situasi yang tidak teratur, di mana keadaan ini bisa terjadi jika ada masukan yang tidak semestinya masuk ke dalam sistem.
3. Kontrol digunakan untuk mencegah, mendeteksi dan memperbaiki situasi yang tidak teratur, sebagai contoh:
    a. Preventive control: instruksi yang diletakkan pada dokumen untuk mencegah kesalahan pemasukan data
    b. Detective control: Kontrol yang diletakkan pada program yang berfungsi mendeteksi kesalahan pemasukan data

c. Corrective control: program yang dibuat khusus untuk memperbaiki kesalahan pada data yang mungkin timbul akibat gangguan pada jaringan, komputer ataupun kesalahan user.

Secara umum, fungsi dari kontrol adalah untuk menekan kerugian yang mungkin timbul akibat kejadian yang tidak diharapkan yang mungkin terjadi pada sebuah sistem. Tugas auditor adalah untuk menetapkan apakah kontrol sudah berjalan sesuai dengan yang diharapkan untuk mencegah terjadinya situasi yang tidak diharapkan. Auditor harus dapat memastikan bahwa setidaknya ada satu buah kontrol yang dapat menangani risiko bila risiko tersebut benar-benar terjadi. Para auditor sistem informasi secara khusus berkonsentrasi pada evaluasi kehandalan atau efektifitas pengendalian / kontrol sistem.

2.1.1 Control Audit Sistem Informasi

Control Audit Sistem Informasi terdiri dari:

1. Kontrol lingkungan (Environmental controls)
   Pengendalian lingkungan meliputi hal-hal seperti kebijakan keamanan IS, standar, dan pedoman; struktur pelaporan dalam lingkungan pemrosesan IS (termasuk operasi komputer dan pemrograman); kondisi keuangan organisasi dan vendor jasa
2. Kontrol keamanan fisik (Physical security controls)
   Kontrol keamanan fisik berkaitan dengan perlindungan terhadap perangkat keras komputer, komponen, dan fasilitas di mana mereka berada.
3. Kontrol keamanan logis (Logical security controls)
   Kontrol keamanan logis adalah yang telah dikerahkan dalam sistem operasi dan aplikasi untuk membantu mencegah akses tidak sah dan penghancuran yang disengaja atau disengaja terhadap program dan data.
4. Kontrol operasi IS (IS operating controls)
   Kontrol operasi sistem informasi, yang dirancang untuk membantu memastikan bahwa sistem informasi beroperasi secara efisien dan efektif. Kontrol ini termasuk penyelesaian tepat waktu dan akurat

pekerjaan produksi, distribusi media output, kinerja cadangan dan prosedur pemulihan, kinerja prosedur pemeliharaan.

2.1.2 Faktor – Faktor Kontrol dan Audit

Faktor-faktor yang mendorong pentingnya kontrol dan audit sistem informasi (Weber, 1999, p.6) adalah antara lain untuk:

1. Mendeteksi agar komputer tidak dikelola secara kurang terarah
2. Mendeteksi risiko kehilangan data
3. Mendeteksi risiko pengambilan keputusan yang salah akibat informasi hasil proses sistem komputerisasi salah/lambat/tidak lengkap.
4. Menjaga aset perusahaan karena nilai hardware, software dan personil yang lazimnya tinggi.
5. Mendeteksi risiko error komputer.
6. Mendeteksi risiko penyalahgunaan komputer (fraud).
7. Menjaga kerahasiaan
8. Meningkatkan pengendalian evalusi penggunaan komputer

2.2 Definisi Audit Sistem Informasi.

Pengertian Audit adalah aktivitas pengumpulan dan pemeriksaan bukti terkait suatu informasi untuk menentukan dan membuat laporan tentang tingkat kesesuaian antara informasi dengan kriteria yang ditetapkan.

Suatu proses sistematis mendapatkan dan mengevaluasi bukti-bukti secara objektif sehubungan dengan asersi atas tindakandan peristiwa ekonomi untuk memastikan tingkat kesesuaian antara asersi-asersi tersebut danmenetapkan kriteria serta mengkomunikasikan hasilnya kepada pihak - pihak yang berkepentingan (Messi eret al, 2006).

Audit pada dasarnya adalah proses sistematis dan objektif dalam memperoleh dan mengevaluasi bukti bukti tindakan ekonomi, guna memberikan asersi/ pernyataan dan menilai seberapa jauh tindakan ekonomi sudah sesuai dengan kretaria yang berlaku dan mengkomunikasikan hasilnya kepada pihak yang terkait (Wardani, 2014).

Audit adalah: Suatu proses sistematik untuk memperoleh dan mengevaluasi bukti secara objektif mengenai pernyataan-pernyataan tentang kegiatan dan kejadian ekonomi, dengan tujuan untuk menetapkan tingkat kesesuaian antara pernyataan- pernyataan tersebut dengan kriteria yang telah ditetapkan, serta penyampaian hasil- hasilnya kepada pemakai yang berkepentingan (Mulyadi ,2014).

Pada awal konsep / bidang kontrol internal mungkin hanya merupakan mekanisme yang sangat tinggi dari segi pandang manajemen perusahaan yaitu sebagai sistem yang dapat ,menjamin dipatuhinya kebijakan perusahaan oleh para pegawai, melindungi aset perusahaan, dan menghindari terjadinya kesalahan / kekeliruan dan penyalahgunaan.

Audit sistem informasi adalah proses pengumpulan dan evaluasi bukti-bukti untuk menentukan apakah sistem komputer yang digunakan telah dapat melindungi aset milik organisasi, mampu menjaga integritas data, dapat membantu pencapaian tujuan organisasi secara efektif, serta menggunakan sumber daya yang dimiliki secara efisien (Weber dalam Yaner, Tanuwijaya, & Sutomo, 2018).

Pengertian sistem Sistem adalah kumpulan dari elemen-elemen berupa data, jaringan data, jaringan kerja dari prosedur-prosedur yang saling berhubungan, sumber daya manusia, teknologi baik hardware maupun software yang saling berinteraksi sebagai satu kesatuan untuk mencapai tujuan/sasaran tertentu yang sama (Maniah dan Dini Hamidin, 2017).

Pengertian Audit Sistem Informasi Beberapa ahli mengemukakan bahwa pengertian audit sistem informasi adalah sebagai berikut:

1. Audit sistem informasi adalah kegiatan yang dilakukan dengan tujuan untuk menilai apakah pengendalian sistem informasi telah dapat memberikan keyakinan yang memadai atas pengamanan aset, integritas data, efektivitas, dan efisiensi.(I Putu Agus Swastika dan Lanang Agung Raditya Putra 2016),
2. Audit sistem informasi adalah proses pengumpulan dan evaluasi buktibukti untuk menentukan apakah sistem komputer yang digunakan telah pencapaian tujuan organisasi secara efektif, serta menggunakan sumber daya yang dimiliki secara efisien. (Tata Sutabri ,2012)
3. Audit sistem informasi adalah pemeriksaan atau audit yang dilaksanakan dalam rangka IT Governance, merupakan audit

operasional secara khusus terhadap pengelolaan sumber daya informasi (Sanyoto Gondodiyoto, 2007).

Secara umum audit teknologi informasi dimaksudkan untuk mengevaluasi tingkat kesesuaian antara teknologi informasi dengan prosedur bisnis (business processes) perusahaan, untuk mengetahui apakah suatu teknologi informasi telah didesain dan diimplementasikan secara efektif, efisien, dan ekonomis. Sehingga, memiliki mekanisme pengamanan aset, serta menjamin integritas data yang memadai (Gondodiyoto, 2017).

Audit Teknologi Informasi adalah mengevaluasi dan mengumpulkan bukti dari adanya sebuah sistem komputer untuk menjaga integritas data serta melindungi sistem komputer yang digunakan. Integritas data yang dijaga merupakan aset perusahaan dalam mencapai tujuan perusahaan secara efektif dan menggunakan sumber daya yang ada. Audit Teknologi Informasi mencakup berbagai macam ilmu yang menjadi suatu kesatuan, diantaranya Traditional Audit, Manajemen Sistem Informasi, Sistem Informasi Akuntasi, Ilmu Komputer, dan Behavioral Science (Isa, 2012a).

2.2.1 Langkah – langkah Audit Sistem Informasi

Proses audit sistem informasi adalah proses yang berkaitan langsung dengan kompleksitas. Terkadang auditor harus menyelesaikan tugasnya dalam sistem yang sangat banyak dan kompleks. Karena kompleksitas merupakan akar permasalahan dari setiap problem yang dihadapai oleh para profesional, maka para ilmuwan telah berusaha untuk membuat panduan untuk mengurangi kompleksitas tersebut, yaitu:

1. Memecah sebuah sistem yang besar menjadi beberapa subsistem untuk dievaluasi secara terpisah
2. Menentukan kehandalan setiap subsistem dan pengaruh setiap subsistem terhadap kehandalan sistem secara keseluruhan

2.2.2 Tahapan Audit

Dalam melakukan kegiatan audit, penelit memakai tahapan audit sebagai berikut:

1. Planning, mendapatkan pemahaman yang lengkap mengenai bisnis perusahaan yang sedang dilakukan audit. Pada proses ini auditor menentukan ruanglingkup dan tujuan pengendalian, tingkat

materialitas, dan outsourcing. Pada tahap ini auditor menetapkan mengapa, bagaimana, kapan dan oleh siapa audit akan dilaksanakan. Untuk mematangkan tahap perencanaan, sebuah program audit awal dipersiapkan untuk menunjukkan sifat, keluasan, dan waktu prosedur-prosedur yang dibutuhkan untuk mencapai tujuan audit dan untuk meminimalkan risiko-risiko audit.

2. Prepare Audit Program, audit program disesuaikan dengan hardware dan software yang dimiliki perusahaan, topologi dan arsitektur jaringan, dan lingkungan serta pertimbangan khusus mengenai industri tersebut. Komponen- komponen dari audit program tersebut adalah: ruang lingkup audit, sasaran audit, prosedur audit, dan rincian administratif (perencanaan dan pelaporan).
3. Gather Evidence, bertujuan untuk mendapatkan bukti-bukti memadai, handal, relevan, dan berguna untuk mencapai sasaran audit secara efektif. Jenis bukti yang sering ditemukan auditor pada kerja lapangan yaitu: observasi proses-proses dan keberadaan dari item fisik seperi pengoperasian komputer atau prosedur backup data, bukti dalam bentuk dokumen (seperti program change logs, sistem access logs, dan tabel otoritas), gambaran dari perusahaan seperi flowcharts, narratives, dan kebijakan dan prosedur yang tertulis), serta analisa seperti prosedur CAATs yang dijalankan pada data perusahaan.
4. Form Conclusion, mengevaluasi bukti- bukti dan membuat suatu kesimpulan tentang hasil pemeriksaan yang pada akhirnya akan mengarah pada opini audit. Auditor juga akan melaporkan kelemahan dan kelebihan darisistem.
5. Deliver Audit Opinion, informasi umum yang harus ada dalam sebuah laporan audit yaitu:
    a. Nama dari organisasi/perusahaan yang diaudit
    b. Judul, tanda tangan, dan tanggal
    c. Pernyataan sasaran audit dan apakah audit tersebut telah memenuhi sasaran

d. Ruang lingkup audit, termasuk di dalamnya area audit fungsional, periode audit yang tercakup, dan sistem informasi, aplikasi, atau lingkungan proses yang diaudit
e. Pernyataan bahwa telah terjadi pembatasan ruang lingkup di mana auditor tidak dapat melaksanakan pekerjaan audit dengan memadai untuk mencapai sasaran-sasaran audit tertentu
f. Pengguna laporan audit yang dikehendaki, termasuk beberapa pembatasan dalam pendistribusian laporan audit
g. Standar-standar dan kriteria yang menjadi dasar auditor untuk melaksanakan pekerjaan audit tersebut
h. Penjelasan rinci mengenai temuan- temuan penting
i. Kesimpulan dari area audit yang dievaluasi, termasuk di dalamnya syarat dan kualifikasi penting
j. Saran-saran yang tepat untuk tindakan perbaikan danpeningkatan
k. Peristiwa-peristiwa penting yang terjadi setelah masa fieldwork audit yang bersangkutan berakhir

6. Follow Up, melakukan tindak lanjut dengan membuat suatu ketentuan untuk melakukan tindak lanjut bersama dengan perusahaan pada kondisi-kondisi yang dilaporkan atau defisiensi audit yang tidak ter-cover selama kegiatan audit. Tindak lanjut ini dapat dilakukan dengan menelepon pihak menejemen.

2.2.3 Tahapan Audit Sistem Informasi

Berikut ini terdapat beberapa tahapan audit sistem informasi, terdiri atas:

1. Perencanaan Audit (Planning The Audit)
   Perencanaan merupakan fase pertama dari kegiatan audit, bagi auditor eksternal hal ini artinya adalah melakukan investigasi terhadap klien untuk mengetahui apakah pekerjaan mengaudit dapat diterima, menempatkan staff audit, menghasilkan perjanjian audit, menghasilkan informasi latar belakang klien, mengerti tentang masalah hukum klien dan melakukan analisa tentang prosedur yang ada untuk mengerti tentang bisnis klien dan mengidentifikasikan risiko audit.

2. Pengujian Pengendalian (Test Of Controls)
   Auditor melakukan kontrol test ketika mereka menilai bahwa kontrol risiko berada pada level kurang dari maksimum, mereka mengandalkan kontrol sebagai dasar untuk mengurangi biaya testing. Sampai pada fase ini auditor tidak mengetahui apakah identifikasi kontrol telah berjalan dengan efektif, oleh karena itu diperlukan evaluasi yang spesifik.
3. Pengujian Transaksi (Test Of Transaction)
   Auditor menggunakan test terhadap transaksi untuk mengevaluasi apakah kesalahan atau proses yang tidak biasa terjadi pada transaksi yang mengakibatkan kesalahan pencatatan material pada laporan keuangan. Tes transaksi ini termasuk menelusuri jurnal dari sumber dokumen, memeriksa file dan mengecek keakuratan.
4. Pengujian Keseimbangan atau Keseluruhan Hasil (Tests Of Balances or Overal Result)
   Untuk mengetahui pendekatan yang digunakan pada fase ini, yang harus diperhatikan adalah pengamatan harta dan kesatuan data. Beberapa jenis subtantif tes yang digunakan adalah konfirmasi piutang, perhitungan fisik persediaan dan perhitungan ulang aktiva tetap.
5. Penyelesaian / Pengakhiran Audit (Completion Of The Audit)
   Pada fase akhir audit, eksternal audit akan menjalankan beberapa test tambahan terhadap bukti yang ada agar dapat dijadikan laporan.
6. Lingkup Audit Sistem Informasi pada umumnya difokuskan kepada seluruh sumber daya sistem informasi yang ada, yaitu Aplikasi, Informasi, Infrastruktur dan Personil.

2.2.4 Tujuan Audit Sistem Informasi

Tujuan audit sistem informasi menurut Ron Weber "1999:11-13" secara garis besar terbagi menjadi empat tahap yaitu:

1. Pengamanan Aset
   Aset informasi suatu perusahaan seperti perangkat keras "hardware", perangkat lunak "software", sumber daya manusia, file data harus

dijaga oleh suatu sistem pengendalian intern yang baik agar tidak terjadi penyalahgunaan aset perusahaan. Dengan demikian sistem pengamanan aset merupakan suatu hal yang sangat penting yang harus dipenuhi oleh perusahaan.

2. Menjaga Integritas Data
   Integritas data "data integrity" adalah salah satu konsep dasar sistem informasi. Data memiliki atribut-atribut tertentu seperti: kelengkapan, kebenaran dan keakuratan. Jika integritas data tidak terpelihara maka suatu perusahaan tidak akan lagi memiliki hasil atau laporan yang benar bahkan perusahaan dapat menderita kerugian.
3. Efektivitas Sistem
   Efektivitas sistem informasi perusahaan memiliki peranan penting dalam proses pengambilan keputusan, suatu sistem informasi dapat dikatakan efektif bila sistem informasi tersebut telah sesuai dengan kebutuhan user.
4. Efisiensi Sistem
   Efisiensi menjadi hal yang sangat penting ketika suatu komputer tidak lagi memiliki kapasitas yang memadai atau harus mengevaluasi apakah efisiensi sistem masih memadai atau harus menambah sumber daya karena suatu sistem dapat dikatakan efisien jika sistem informasi dapat memenuhi kebutuhan user dengan sumber daya informasi yang minimal.
5. Ekonomis
   Ekonomis mencerminkan kalkulasi untuk rugi ekonomi "cost/benefit" yang lebih bersifat kuantifikasi nilai moneter "uang". Efisiensi berarti sumber daya minimum untuk mencapai hasil maksimal. Sedangkan ekonomis lebih bersifat pertimbangan ekonomi.
6. Ketersediaan.
   Berhubungan dengan ketersediaan dukukan/layanan teknologi informasi TI.TI hendaknya dapat dapat mendukung secara kontinyu terhadap proses bisnis.Semakin sering terjadi gangguan maka berarti tingkat ketersediann sistem rendah.

7. Kerahasian.
   Fokusnya pada proteksi terhadap informasi dan supaya terlindung dari akses dari pihak-pihak yang tidak berwenang.
8. Kehandalan.
   Kesesuaian dan keakuratan bagi manajemen dalam pengelolaan organisasi, pelaporan dan pertanggunjawaban.
9. Menjaga Intergritas Data
   Integritas data adalah salah satu konsep dasar sistem informasi, data memiliki atribut atribut yaitu: kelengkapan, kebenaran, dan keakuratan.

2.2.5 Keuntungan Audit

1. Menilai keefektifan aktivitas aktivitas dokumentasi dalam organisasi
2. Memonitor kesesuaian dengan kebijakan, sistem, prosedur dan undang-undang perusahaan
3. Mengukur tingkat efektifitas dari sistem
4. Mengidentifikasi kelemahan di sistem yang mungkin mengakibatkan ketidak sesuaian di masa datang
5. Menyediakan informasi untuk proses peningkatan
6. Meningkatkan saling memahami antar departemen dan antar individu
7. Melaporkan hasil tinjauan dan tindakan berdasarkan risiko ke Manajemen.

2.2.6 Tinjauan Penting dalam Audit SI / TI

Adapun elemen utama dari aktivitas peninjauan yang dilakukan dalam Audit SI/TI dapat dikalfikasikan kedalam tinjaunan penting sebagai berikut:

a. Tinjauan terkait dengan fisik dan lingkungan yakni: hal hal yang terkait dengan kemanan fisik, suplai sumber daya , temperatur, kontrol kelembaban dan faktor lingkungan lain.
b. Tinjauan administrasi sistem yaitu mencakup tinjaun keamanan sistem operasi, sistem manajemen database, seluruh prosedure administrasi sistem dan pelaksanannya.

c. Tinjauan perangkat lunak . Perangkat lunak yang dimaksud merupakan aplikasi bisnis yang dapat berupa sistem berbasis web untuk pemrosesan permintaan pelanggan hingga Enterprise Reasource Planining (ERP) yang kini menjadi inti dari proses bisnis diperusahaan
d. Tinjauan keamanan jaringan yang mencakup tinjauan jaringan internal dan eksternal yang terhubung dengan sistem, batasan tingkat keamanan, tinjauan terhadap firewall, daftar kontrol akses router, prort scaning serta pendeteksian akan gangguan maupun ancaman terhadap sistem.
e. Tinjaunan kontinuitas bisnis dengan memastikan ketersediaan prosedur backup dan menyimpanan, dokumentasi dari prosedur tersebut serta dokumentasi pemulihan bencana/ kontinuitas bisnis yang dimiliki.
f. Tinjauan intergritas data yang bertujuan untuk memastikan ketelitian data beroperasi sehingga dilakukan verifikasi kecukupan kontrol dan dampak dari kurangnya kontrol yang ditetapkan.

2.3 Pengertian Motivasi

Pengertian Motivasi Kata Motivasi berasal dari kata Latin "Motive" yang berarti dorongan, daya penggerak atau kekuatan yang terdapat dalam diri organism yang menyebabkan organism itu bertindak atau berbuat. Selanjutnya diserap dalam bahasa Inggris motivation berarti pemberian motiv, penimbulan motiv atau hal yang menimbulkan dorongan atau keadaan yang menimbulkan dorongan.

Menurut Landy dan Becker (2011:59) pengertian motivasi adalah: "The term motivation has at least two connotations in the field organization behavior, the first is a management process, used this way. Motivation is seen as a management activity, something that management do to induce others to act in a way to produce result desired by organization or perhaps by the manager. In this context we might say role of every manager is to motivate employee to work harder or to do betteras a psychological concept motivation refers to internal mental state of a person, which relates to the initiation, direction, persistence intensity and termination of behavior." Dalam pernyataan Landy dan Becker

menjelaskan bahwa Istilah motivasi setidaknya memiliki dua konotasi dalam perilaku organisasi lapangan, yang pertama adalah proses manajemen, yang digunakan dengan cara ini. Motivasi dipandang sebagai kegiatan manajemen, sesuatu yang dilakukan manajemen untuk mendorong orang lain bertindak dengan cara menghasilkan hasil yang diinginkan oleh organisasi atau mungkin oleh manajer. Dalam konteks ini kita bisa mengatakan peran setiap manajer adalah memotivasi karyawan untuk bekerja lebih keras atau melakukan yang lebih baik sebagai motivasi konsep 24 psikologis mengacu pada keadaan mental internal seseorang, yang berkaitan dengan inisiasi, arahan, intensitas ketekunan dan penghentian perilaku.

2.4 Tujuan Audit Sistem Informasi Dan Keuntungan Diaudit, Jenis Audit

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

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

Menurut Gallegos dalam bukunya "Audit And Control Of Information System" menyatakan audit sistem informasi meliputi beberapa tahapan yakni:

1. Perencanaan (Planning) Meliputi aktivitas utama, yakni:
   a. Menetapkan ruang lingkup dan tujuan audit
   b. Mengorganisasikan tim audit
   c. Memahami tentang oprasi bisnis klien
   d. Mengkaji ualgn hasil audit sebelumnya
   e. Menyiapkan program audit

2. Pemeriksaan Lapangan (Field Work)
   Pada tahap ini yang dikerjakan yaitu mengumpulkan informasi yang dilakukan dengan cara mengumpujlkan data dengan pihak-pihak yang berhubungan. Hal ini bisa dilakukan dengan cara penerapan metode pengumpulan data yakni wawancara, quisioner atau melakukan survey.
3. Pelaporan (Reporting)
   Setelah pengumpulan data, maka akan diperoleh data yang akan diproses untuk dihitung menurut perhitungan maturity level. Di tahapan ini akan dilakukan pemberian informasi dalam bentuk hasil-hasil dari audit.

4. Tindak Lanjut (Follow Up)
   Tahapan ini dilakukan dengan pemberian laporan hasil audit dalam bentuk rekomendasi tindakan perbaikan kepada pihak manajemen objek yang diteliti, untuk kemudian wewenang perbaikan menjadi tanggung jawah manajemen objek yang diteliti apakah akan diterapkan atau hanya menjadi acuan untuk perbaikan di masa yang akan datang

Bab 3

Pendekatan Audit Sistem Informasi

3.1 Jenis Pendekatan Audit Sistem Informasi

1. Pendekatan temuan (Exposures Approach)
2. Pendekatan Kendali (Control Approach)
   Pesatnya perkembangan dunia komputer , diikuti dengan peningkatan penegetahuan auditor, ternyata mengandung dua perlakuan terhadap komputer , yaitu:
   a. Komputer dipergunakan sebagai alat bantu auditor dalam melaksanakan audit.
   b. Komputer dijadikan sebagai target audit, karena data di entry ke komputer dan hasilnya untuk menilai kehandalan pemrosesan dan keakuratan komputer.

Audit TI sendiri merupakan gabungan dari berbagai macam ilmu, antara lain: Traditional Audit, Manajemen Sistem Informasi, Sistem Informasi Akuntansi, Ilmu Komputer, dan Behavioral Science.

3.2 Jenis Audit Sistem Informasi

Jenis audit Sistem Informasi /Teknologi Informasi antara lain:

1. System Audit Audit terhadap sistem terdokumentasi untuk memastikan sudah memenuhi standar nasional atau internasional
2. Compliance Audit Untuk menguji efektivitas implementasi dari kebijakan, prosedur, kontrol dan unsur hukum yang lain
3. Product/Service Audit Untuk menguji suatu produk atau layanan telah sesuai seperti spesifikasi yang telah ditentukan dan cocok digunakan

3.3 Kelompok Pendekatan Audit Sistem Informasi

Dalam berjalannya evolusi tersebut, maka munculah pendekatan audit sistem informasi yang dapat dikategorikan kedalam tiga kelompok:

1. Auditing around the computer

   Dalam pendekatan audit di sekitar komputer, auditor (dalam hal ini harus akuntan yang registered, dan bersertifikasi akuntan publik) dapat mengambil kesimpulan dan merumuskan opini dengan hanya menelaah struktur pengendalian dan melaksanakan pengujian transaksi dan prosedur verifikasi saldo perkiraan dengan cara sama seperti pada sistem akuntansi manual. Kunci pendekatan audit ini ialah pada penelusuran transaksi terpilih mulai dari dokumen sumber sampai ke bagan-perkiraan (akun) dan laporannya. Keunggulan metode audit di sekitar komputer adalah:

   a. Pelaksanaan audit lebih sederhana.
      Auditor yang memiliki pengetahuan minimal di bidang komputer dapat dilatih dengan mudah untuk melaksanakan audit.
   b. Kelemahannya adalah jika kondisi (user requirements) berubah, mungkin sistem itupun perlu diredesain dan perlu penyesuaian (update) program- program, bahkan mungkin struktur data/file,

sehingga auditor perlu menilai/menelaah ulang apakah sistem masih berjalan dengan baik.

2. Audit with the computer
   Audit dengan komputer untuk kegiatan pendukung dan administrasi paling sering digunakan, bahkan meskipun sistem klien yang diaudit telah berbasis komputer. Selain untuk kegiatan administratif, penyusunan program audit dan kuesioner serta pencatatan-pencatatan dan pelaporan hasil audit, komputer biasanya juga digunakan oleh auditor atau pegawai perusahaan klien untuk melakukan analisis atau pengikgtisaran, pembuatan grafik dan tabel-tabel tentang hasil audit, sertapemaparan atau presentasi hasil audit (misalnya dengan Microsoft Word, PowerPoint, dan Excel).
3. Audit throught the computer
   Dalam pendekatan audit ke sistem komputer (audit through the computer) auditor melakukan pemeriksaan langsung terhadap program-program dan file- file komputer pada audit SI berbasis TI. Auditor menggunakan komputer (software) atau dengan cek logika atau listing program (desk test on logic or programs source code) untuk menguji logika program dalam rangka prngujian pengendalianyang ada pada komputer. Selain itu auditor juga dapat meminta penjelasan dari para teknisi komputer mengenai spefikasi sistem dan/atau program yang diaudit.
4. Keunggulan pendekatan audit dengan pemeriksaan sistem komputerisasi, ialah:
   a. Auditor memperoleh kemampuan yang besar dan efektif dalam melakukan pengujian terhadap sistem komputer.
   b. Auditor akan merasa lebih yakin terhadap kebenaran hasil kerjanya.
   c. Auditor dapat menilai kemampuan sistem komputer tersebut untuk menghadapi perubahan lingkungan

Ada 3 kategori strategi ketika Auditing Through the computer, yaitu:

1. Test data approach (Test data)
   Metode ini menggunakan data masukan yang telah dipersiapkan auditor dan menguji data tersebut dengan salinan (copy) dari perangkat lunak aplikasi auditan. Hasil pemrosesan data tersebut akan dibandingkan dengan ekspektasi auditor. Jika ada hasil yang tidak sesuai, mungkin ini suatu indikasi penyimpangan logika atau mekanisme pengendalian.
2. Paralel simulation
   Pendekatan ini mengharuskan auditor untuk membuat suatu program yang menyimulasikan fungsi utama tertentu dari aplikasi yang sedang diuji.Sedangkan untuk melakukan pengujian substantif (misalnya detail transaksi atau saldo perkiraan),makaauditordapatmemilihteknik:
3. Embeded audit module approach
   Merupakan suatu teknik di mana satu atau lebih modul program tertentu dilekatkan di suatu aplikasi untuk mencatat secara tersendiri serangkaian transaksi yang telah ditentukan ke dalam file yang akan dibaca oleh auditor

Dalam Merancang organisasi perusahaan perlu memperhatikan dan dipertimbangkan sistem pengendalian internt sebagai berikut:

1. Struktur organisasi yang memisahkan tanggung jawab fungsional secara tegas.
2. Sistem berwenang dan prosedur pencatatan yang memberikan perlindungan yang cukup terhadap kekayaan, utang, pendapatan, dan biaya.
3. Praktek yang sehat dalam melaksanakan tugas dan fungsi tiap unit organisasi
4. Karyawan yang mutunya sesuai dengan tanggungjawab

3.4 Metode Proses Audit Sistem Informasi

Metode dalam proses Audit SI, dapat dilakukan dengan langkah-langkah sebagai berikut:

1. Metode pemahaman
    a. Mendokumentasikan aktivitas yang mendasari control objective demikian juga untuk mengidentifikasi stade control measure/procedure yang berlaku
    b. .Melakukan wawancara dengan manajemen dan staf untuk mendapatkan pemahaman tentang: kebutuhan bisnis dan risikonya, struktur organisasi, peran dan tanggung jawab, kebijakan procedure, hukum dan peraturan, control measure yang berlaku, laoran manajemen
    c. Mendokumentasikan proses yang berhubungan dengan sumber daya TI terutama yang dipengaruhi oleh proses direview.
2. Evaluasi Kendali
    a. Menilai keefektifan control maesure yg berlaku atau tingkat pencapaian control objective .
    b. Mengevaluasi kesesuaian control measure dari proses yang direview dengan mempertimbangkan kriteria yg diidentifikasikan dan praktik standar industri, Critical Success Factor dan Control measure dan mengaplikasikan keputusan profesional audit.
    c. Melakukan proses dokumentasi, deliverable yang sesuai dihasilkan, tanggung jawab dan akuntabilitas yang jelas dan efektif, adanya pengendalian kompensasi sebagaimana mestinya
    d. Simpulkan sesuai tingkat Control Objective
3. Menilai Kepatuhan
    a. Menjamin control measure yg ditetapkan , berjalan sebagaimana mestinya, secara konsisten dan berkelanjutan, serta menyimpulkan kesesuaian control environment.
    b. Mendapatkan bukti langsung dan tidak langsung untuk item / periode yg dipilih untuk menjamin bahwa prosedur telah dipatuhi

untuk periode yang direview menggunakan alat bukti langsung dan tidak langsung.

c. Melakukan review terbatas ttg kecukupan proses deliverable.
d. Menentukan tingkat pengujian substatif dan kerja tambahan yg dibutuhkan unt menyediakan jaminan proses IT adalah cukup.

4. Penilaian Risiko.
   a. Memperkirakan risiko dari control objective yg tidak dipenuhi, dengan menggunakan teknik analitik dan atau mengkonsultasikan sumber sumber alternative.
   b. Mendokumentasikan kelemahan kendali, serta ancaman dan kerawanan yang dihasilkan.
   c. Mengidentifikasikan dan mendokumentasikan dampak yang potensial maupun aktual.
   d. Menyediakan informasi komparatif, misalnya melalui benchmark Secara Garis besar Metodologi dalam Audit SI dan TI akan terdiri atas beberapa tahapan anatara lain:
      - Analisis Kondisi Eksisteing
        Yang merupakan aktivitas dalam memahami kondisi saat ini perusahaan yang diaudit termasuk hukum dan regulasi yang berpengaruh terhadap operasional proses bisnis.
      - Penentuan tingkat risiko
        Dengan mengklasifikasikan proses bisnis yang tingkat risikonya tinggi maupun proses bisnis pendukung. Hasil penentuan tingkat risiko tersebut kemudian dijadikan sebagai bahan dalam penyusunan ruang lingkup pelaksanaan audit yang diarahkan kepada proses bisnis yang didukung oleh TI
      - Pelaksanaan Audit SI/TI dengan mengacu kerangka kerja COBIT yang akan didahului dengan proses penentuan ruang lingkup dan tujuan audit berdasarkan hasil penentuan tingkat risiko pada tahapan sebelumnya.
      - Penentuan rekomendasi beserta laporan dari hasil audit yang dilakukan.

3.4.1 Tinjauan Penting dalam Audit Sistem Informasi

Adapun elemen utama dari aktivitas peninjauan yang dilakukan dalam Audit SI/TI dapat diklasifikasi kedalam tinjauan penting sebagai berikut:

1. Tinjauan terkait dengan fisik dan lingkungan yakni: hal hal yang terkait dengan keamanan fisik, suplai sumber daya, temperatur, kontrol kelembaban dan faktor lingkungan
2. Tinjauan Administrasi sistem yaitu mencakup tinjauan keamanan sistem operasi, sistem manajemen database seluruh prosedur administrasi sistem dan pelaksanaannya.
3. Tinjauan Perangkat Lunak. Perangkat lunak yang dimaksud merupakan aplikasi bisnis yang didaat berupa sistem berbasis web untuk pemrosesan permintaan pelanggan hingga ERP yang kini menjadi inti dari proses bisnis diperusahaan.
4. Tinjauan keamanan jaringan yang mencakup tinjauan jaringan internal dan eksternal yang terhubung dengan sistem, batasan tingkat keamanan, tinjauan terhadap firewall daftar kontrol akses router, port scaning serta pendeteksian akan gangguan maupun ancaman terhadap sistem.
5. Tinjauan Kontinuitas bisnis dengan memastikan ketersediaan prosedur backup dan penyimpanan, dokumentasi dari prosedure tersebut serta dokumentasi pemulihan bencana yang dimiliki.
6. Tinjauan intergritas data yang bertujuan untuk memastikan ketelitian data yang beroperasi sehingga dilakukan verifikasi kecukupan kontrol dan dampak dari kurangnya kontrol yang ditetapkan.

3.5 Konsep Risiko dan Jenis-jenis risiko

3.5.1 Konsep Risiko

Agar segala sesuatu berjalan sesuai yang seharusnya, maka perlu ada pengawasan. Salah satu bentuk/cara pengawasan ialah yang disebut system pengendalian intern (internal control system) yang melekat pada system dan prosedur organisasi tersebut.

Pendekatan Audit SI /TI berbasis risiko digunakan untuk menilai risiko dari poses bisnis yang berlangsung diorganisasi atau perusahaan dan yang terpenting dapat membantu pengaudit SI/TI dalam memutuskan metode pengujian yang digunakan dalm pelaksaaan audit nantinya dengan melakukan uji kepatutan atau uji secara substantif

3.5.2 Jenis Jenis Risiko

Adapun Jenis jenis risiko sebagai berikut:

1. Risiko Bisnis (Bussiness Risks)
   Risiko bisnis adalah risiko yang dapat disebabkan oleh faktor-faktor intern maupun ekstern yang berakibat kemungkinan tidak tercapainya tujuan organisasi (business goals objectives).
   a. Risiko ekstern (risk from external environment) ialah misalnya antara lain perubahan kondisi perekonomian tingkat kurs yang berubah mendadak, dan munculnya pesaing baru yang mempunyai potensi bersaing tinggi
   b. Risiko internal ialah risiko yang berasal dari internal misalnya antara lain permasalahan kepegawaian, risiko-risiko yang berkaitan dengan peralatan atau mesin, risiko keputusan yang tidak tepat, dan kecurangan manajemen (Manajement Fraud)
2. Risiko Bawaan (Inherent Risks)
   Risiko bawaan ialah potensi kesalahan atau penyalahgunaan yang melekat pada suatu kegiatan, jika tidak ada pengendalian intern. Misalnya kegiatan kampus, apabila tidak ada absensi/daftar kehadiran kuliah akan banyak mahasiswa yang cenderung tidak disiplin hadir mengikuti kuliah. Inherent risk atau risiko bawaan merupakan risiko kesalahan audit yang merupakan aktivitas bawaan dari proses bisnis.Risiko kesalahan tersebut bersifat indenpenden dan akan semakin tinggi jika compensating control tidak tersedia.
3. Risiko Pengendalian (Control Risks)
   Dalam suatu organisasi yang baik seharusnya sudah ada risks assessment, dan dirancang pengendalian intern secara optimal terhadap setiap potensi risiko. Risiko pengendalian ialah masih adanya risiko meskipun sudah ada pengendalian. Control Risk atau risiko

kontrol merupakan risiko kesalahan yang tidak terdeteksi oleh kontrol internal itu sendiri selama proses audit berlangsung. Risiko kontrol tersebut menjadi rendah jika prosedur validasi tersedut dilakukan secaraterkomputerisasi.

Risiko pengendalian tidak pernah mencapai keyakinan penuh bahwa semua salah saji material akan dapat dideteksi ataupun dicegah. Risiko pengendalian merupakan fungsi dari efektivitas struktur pengendalian inter. Semakin efektif struktur pengendalian intern perusahaan klien, semakin kecil risiko pengendaliannya. Penetapan risiko pengendalian didasarkan atas kecukupan bukti audit yang menyatakan bahwa struktur pengendalian inter klien adalah efektif. Ada dua macam risiko pengendalian, yaitu:

1. Actual level of control risk Assessed level of control risk yang ditentukan dengan melakukan modifikasi prosedur untuk menghimpun pemahaman struktur pengendalian intern terkait dengan asersi, dan prosedur untuk melaksanakan test of control. Pada saat perencanaan audit, auditor menentukan besarnya risiko pengendalian yang direncanakan untuk setiap asersi yang signifikan.

   Planned assessed level of control risk ini ditentukan berdasar asumsi tentang efektivitas rancangan dan operasi struktur pengendalian intern yang relevan.
2. Risiko Deteksi (Detection Risks)

   Risiko deteksi adalah risiko yang terjadi karena prosedur audit yang dilakukan mungkin tidak dapat mendeteksi adanya error yang cukup materialitas atau adanya kemungkinan fraud. Risiko deteksi mungkin dapat terjadi karena auditor ternyata dalam prosedur auditnya tidak dapat mendeteksi terjadinya existing control failures (system pengendalian intern yang ada ternyata tidak berjalan baik).
3. Audit (Audit Risks)

   Risiko audit sebenarnya adalah kombinasi dari inherent risks, control risks, dan detection risks. Risiko audit adalah risiko bahwa hasil pemeriksaan auditornya ternyata belum dapat mencerminkan keadaan yang sesungguhnya.

4. Ada Pun rumus mengetahui Risiko Audit dengan rumus di bawah:
   Model Risiko Audit (audit risk) yang paling lumrah digunakan (dan diajarkan) adalah: AR = IR x CR x DR

Di mana:
AR = Audit Risk IR = Inherent Risk
CR = Control Risk DR = Detection Risk
Mengenai jenis – jenis risiko, dalam bukunya yang berjudul Accounting Information System, F.L. Jones dan D.V. Rama (2003,p127-134) tidak membahas masalah business risk, tetapi menyebut risiko – pelaksanaan (execution risks) yang mungkin lebih sempit ruang lingkupnya. Jones dan Rama berpendapat risiko pada hakekatnya dapat dikelompokkan kedalam 4 jenis risiko, yaitu execution risks, information risks, asset protection risks, dan performance risks.

1. Execution risk
   Execution risk adalah risiko yang berkaitan dengan tidak tercapainya sesuatu yang seharusnya dilaksanakan.
2. Information risk
   Risiko informasi yang dimaksud oleh Jones dan Rama ini ialah risiko yang berkaitan dengan kemungkinan kesalahan atau penyalahgunaan data informasi. Risiko terjadi waktu mencatat/entri data (recording risks) serta updating risks.
3. Asset protection risk
   Risiko yang berkaitan dengan save guarding assets ini ialah kerusakan, hilang, atau asset tidak digunakan seperti yang seharusnya, maupun risiko yang dapat timbul terhadap assets perusahaan akibat keputusan yang salah.
4. Performance Risk
   Risiko kinerja ini adalah risiko berkaitan dengan kinerja pegawai/ kinerja perusahaan yang tidak dapat dilaksanakan sesuai tujuan/standar/ukuran yang ditetapkan. Pada hakekatnya yang bertanggung jawab dan akan mempertanggung jawabkan pengelolaan perusahaan kepada para share/stockholder dan stakeholder adalah para pengurus perusahaan, yang menurut Undang-undang Perseroan Terbatas di Indonesia ialah para anggota Dewan Direksi dan anggota Dewan Komisaris.

Dalam pelaksanaan kegiatan sehari-hari, yang melakukan tugas operasional ialah para manajer tingkat menengah, supervisor, staf dan pegawai pelaksana, yang melaksanakan tugas sesuai dengan kebijakan yang ditetapkan pimpinan. Jika mereka tidak melakukan tugas sesuai dengan yang seharusnya, atau kalau kinerjanya tidak sesuai dengan yang seharusnya. Hal ini merupakan risiko yang dipreventif, dideteksi, atau dikoreksi/diperbaiki. Audit risiko merupakan risiko kemungkinan auditor ekstern memberikan opini yang salah terhadap fairness laporan keuangan auditee, atau temuan dan rekomendasi yang salah pada laporan hasil pemeriksaan auditor intern. Risiko ini sangat berbahaya karena auditor sudah memberikan opini atau rekomendasi bahwa "Things are okay and fine, but they are not"

Efek Risiko dalam sistem informasi ditemui pada:

1. Strategi (Strategic): risiko di mana sistem informasi tidak sesuai dengan tujuan organisasi dan tidak mendukung pencapaian misi.
2. Operasi (Operations): risiko di mana sistem informasi menimbulkan beban yang terlalu besar bagi organisasi. Selain itu ketergantungan organisasi terhadap suatu sistem informasi berarti apabila sistem tersebut tidak tersedia selama waktu tertentu dapat menimbulkan risiko besar bagi operasional.
3. Pelaporan (Reporting): risiko di mana sistem informasi tidak dapat diandalkan untuk menghasilkan informasi yang akurat, lengkap dan tepat waktu.
4. Kepatuhan (Compliance): risiko di mana sistem informasi malah menimbulkan pelanggaran hukum dan regulasi yang merugikan bagi organisasi baik secara finansial maupun reputasi.
5. Keterkaiatan antar Tujuan Bisnis dan TI akan dipaparkan dengan mengacu pada kerangka kerja COBIT. Kerangka kerja tersebut memberikan pemetaan keterkaitan antara tujuan bisnis dengan tujuan TI sehingga dapat dijadikan acuan bagi perusahaan dalam menerjemakan kebutuhan bisnis akan tersediaan TI.

Bab 4

Sistem Pengendali Audit Sistem Informasi

4.1 Pengertian Sistem Pengendalian Internal

Dari beberapa referensi yang kita pelajari kita dapat mengetahui bahwa sampai pada awal abad 19 terminologi Internal Control System belum merupakan konsep yang dipahami meluas. Sebelumnya yang lebih dikenal adalah internal check, maksudnya ialah kegiatan klerikal pemeriksaan akurasi (kecermatan) book keeping yang pada saat ini lazimnya disebut verifikasi "independen" (pemeriksaan ulang secara independen, artinya orang atau unit lain bukan yang mengerjakan pertama).

Sistem Pengendalian Internal (Internal Control System) dalam sistem informasi dapat di kelompokkan dalam beberapa kategori, berdasarkan Jenis:

1. Reventive Detective, Dan Corrective (Pencegahan, Deteksi Dan Koreksi)
2. Discretionary Dan Non-discretinary (Kebikjakan Dan Kebebasan)
3. Volumtary Dan Mandated (Sukarela Atau Diwajibkan)
4. Manual Atau Automated (Control Secara Manual Atau Dengan Computer)
5. Kontrol Perspektif Manajemen Dan Perspektif Teknis
6. Application Dan General Controls.

Menurut Gramling, Ri0enberg, dan Johnstone (2012: 208), *"Internal control is a process related to the achievement of the organiza5on' s objec5ves. Organiza5ons iden5fy the risks to achieving those objec5ves and implement various controls to mi5gate those risks"*. Pengendalian internal diperlukan untuk mengidentifikasi risiko agar proses bisnis perusahaan tidak terganggu.

Pengendalian Internal adalah Pengendalian dalam suatu organisasi bertujuan untk menjaga aset perusahaan, pemenuhan terhadap kebijakan dan prosedur, kehandalan dalam proses dan operasi yang efesien.

4.1.1 Tujuan Pengendalian internal.

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

1. Meningkatkan pengamanan (improve safeguard) aset sistem informasi (data/catatan akuntansi (accoun5ng records) yang bersifat logical assets, maupun physical assets seperti hardware, infrastructures, dan sebagainya).
2. Meningkatkan integritas data (improve data integrity), sehingga dengan data yang benar dan konsisten akan dapat dibuat laporan yang benar.
3. Meningkatkan efekAfitas sistem (improve system effec5veness).
4. Meningkatkan efisiensi sistem (improve system efficiency).

Tujuan sistem pengendalian internal direncanakan atau dirancang dengan tujuan untuk:

1. Menjaga kekayaan organisasi,
2. Mengecek keteliAan dan kehandalan data akuntasi,
3. Mendorong efisiensi,
4. Mendorong dipatuhinya kebijakan manajemen

4.2 Sistem Pengendalian Umum

Menurut Sawyer, Dioenhofer, & Scheiner (2005), *general control consist of those controls in the IS and user environment that are pervasive over all or most applica5on. They include such controls as segrega5on of incompa5ble du5es,*

system development procedures, data security, all administra5ve controls, and disaster recovery capabili5es.

Pengendalian umum didefinisikan sebagai sistem pengendalian internal komputer yang berlaku umum meliputi seluruh kegiatan komputerisasi sebuah organisasi secara menyeluruh. Artinya ketentuan – ketentuan dalam pengendalian tersebut berlaku untuk seluruh kegiatan komputerisasi yang digunakan di perusahaan tersebut.

Sistem pengendalian Umum yaitu manajemen menetapkan kebijakan yang dirumuskan untuk melaksanakan di dalam organisasi atau perusahaan, setiap orang melaksanakan kebijakan ini dengan memberikan tanggung jawab untuk setiap pekerjaannya, dalam batasan yang telah ditetapkan dalam suatu peraturan. Pengendalian umum (general control) adalah sistem pengendalian intern computer yang berlaku umum meliputi seluruh kegiatan komputerisasi sebuah organisasi secara menyeluruh. artinya ketentuan– ketentuan yang di atur dalam pengendalian intern tersebut berlaku untuk seluruh kegiatan komputerisasi pada organisasi / perusahaan tersebut.

Pengendalian umum adalah merupakan " Payung" atau kebijakan umum pengendalian dalam suatu organisasi, apabila tidak dilakukan pengendalian dapat berakibat negative terhadap aplikasi atau kegiatan komputerisasi organisasi. Pengendalian umum adalah kebijakan umum pengendalian dalam suatu suatu organisasi, apabila tidak dilakukan pengendalian dapat berakibat negative terhadap aplikasi atau kegiatan komputerisasi oraganisasi atau perusahaan. Karena Pengendalian umum mengatur seluruh seluruh kegiatan perusahaan yang berkaitan dengan komputerisasi / teknologi informasi maka keputusan pengendalian jenis ini merupakan wewenang atau domain manajemen (bersifat manajemen framework) dan oleh sebab itu beberapa textbook tidak menggunakan istilah pengendalian umum, melainkan Pengendalian Perspektif Manajemen. Oleh karena pengendalian umum ini menyangkut seluruh kegiatan komputerisasi pada suatu organisasi, maka berwenang menentukan struktur pengendalian adalah pimpinan organisasi tersebut,atau dalam prakteknya wewenang tersebut didelegasikan kepada kepala unit komputer

Ikatan Akutansi Indonesia (IAI,2001,SA319, par.06) mengkelasifikasikan pengendalian umu sebagai berikut:

1. Pengendalian organisasi dan manajemen
2. Pengendalian terhadap pengembangan dan pemeliharaan sistem aplikasi

3. Pengendalian terhadap pengembangan operasi sistem
4. Pengendalian terhadap perangkat lunak sistem
5. Pengendalian terhadap TI (Pengolahan Data Elektronis)

4.2.1 Ruang lingkup Pengendalian Umum

Ruang lingkup yang termasuk dalam pengendalian umum (pengendalian perspektif manajemen) diantaranya adalah :

1. Pengendalian manajemen puncak (top management controls).
2. Pengendalian manajemen pengembangan sistem (information system management controls).
3. Pengendalian manajemen sumber data (data resources management controls).
4. Pengendalian manajemen operasi (operations management controls).
5. Pengendalian manajemen keamanan (security administration Management controls).
6. Pengendalian manajemen jaminan kualitas (quality assurance management controls).

4.3 Jenis-jenis pengendalian

Jenis Pengendalian Umum dan katergori pengendalian:

1. Organisasi dan Manajemen
   a. Pemisahan fungsi Depertemen TI dan Non TI
   b. Pemeriksaan fungsi dalam Depertemen TI
   c. Otorisasi Tranksasi
   d. Pengendalian Porsonil
   e. Perencanaan, Penganggaran dan sistem pembebasan kepada pemakai (user)
2. Piranti Lunak Dan Keras
   a. Pengendalian Piranti Keras (Hardware)
   b. Pengendalian Piranti Lunak (Software)
3. Pengendalian Akses
   a. Pembatasan Akses fisik dan Lojik

   b. Dokumentasi Program
   c. Fasilitas- Fasilitas On-line
4. Data dan Procedur
   a. Control Group
   b. File dan database
   c. Procedur- procedure standar
   d. Keamanan fisik
   e. Pemeriksaan Interen
5. Pengembangan Sistem Baru
   a. Partisipasi manajemen dan Pemakai
   b. Pengembangan Standar & pedoman
   c. Manajemen Proyek
   d. Pengujian sistem dan konversi
   e. Penelaahan setelah pemasangan
6. Pemeriharaan Program
   a. Otorisasi dan persetujuan
   b. Prosedur standar dan dekomentasi
   c. Pengendalian pemrogram dan pelaksanaan
   d. Pengujian terhadap perubahaan
7. Dokumentasi
   a. Dokumentasi standar dan dekomentasi pendefinisian masalah
   b. Dokumentasi sistem
   c. Dokumentasi program
   d. Dokumentasi operasional
   e. Domentasi pemakai 3.4.Pengendalian Pucuk Pimpinan

Pengendalian pucuk pimpinan adalah sistem pengendalian intern yang ada pada suatu organisasi yang mendorong keterlibatan, kepedulian dan tanggung jawab pucuk pimpinan organisasi terhadap kegiatan TI pada organisasi.

Pucuk pimpinan (Top management) adalah board of director atau di sebut direksi, terdiri dari direktur utama dan para direktur lainnya. Direksi bertanggung jawab terhadap seluruh operasi perusahaan, termasuk bidang Teknologi Informasi Bagaimana Auditor menganalisa perhatian / kepedulian top management terhadap fungsi sistem informasi? Salah Satu cara yang dapat di lakukan adalah dengan melihat bagaimana Top Management terkait dengan

sistem Informasi seperti layaknya tugas pokok dan fungsi management pada umumnya.

4.3.1 Fungsi Internal Auditor.

Seorang auditor TI sebaiknya mampu melakukan pekerjaan-pekerjaan sebagai berikut:

1. Mengevaluasi pengendalian atas aplikasi-aplikasi tertentu, yang mencakup analisis
2. terhadap risiko dan pengendalian atas aplikasi-aplikasi seperti e-business, sistem perencanaan sumber daya perusahaan.
3. Memberikan asersi (assurance) atas proses-proses tertentu, sepert audit dengan prosedur-prosedur tertentu yang disepakat bersama dengan auditee mengenai lingkup asersi. Memberikan asersi atas akAfitas pengolahandata pihak ketiga dengan tujuan untuk memberikan asersi bagi pihak lain yang memerlukan informasi mengenai aktivitas pengendalian data yang dilakukan oleh pihak ketiga tersebut.
4. Pengujian penetrasi, yaitu upaya untuk mengakses sumber daya informasi guna menemukan kelemahan-kelemahan yang ada dalam pengolahan data tersebut. Memberikan dukungan atas pekerjaan audit keuangan yang mencakup evaluasi atas risiko dan pengendalian TI yang dapat memengaruhi kehandalan sistem pelaporan keuangan.
5. Mencari kecurangan yang berbasis TI, yaitu menginvestigasi catatan-catatan komputer dalam invesAgasi kecurangan.

4.4 Jenis Perancangan Pengendalian

Top Management bertanggung jawab untuk membuat master-plan sistem informasi, meliputi rencana jangka Panjang& jangka pendek.

Penyusunan Rencana meliputi 3 hal:

1. Mengetahui kesempatan dan masalah yang di hadapi organisasi sehingga teknologi informasi dan system Informasi dapat di gunakan secara efektif.

2. Mengindentifikasi sumber daya yang di perlukan untuk menyedikan Teknologi dan sistem informasi yang di perlukan.
3. Membuat strategi dan takti yang di perlukan untuk memperoleh sumber daya tersebut

Jenis perancangan pengendalian dibedakan dalam 2 jenis, yaitu:

1. Strategi Plan
   Strategi Plan bersifat jangka anjang dan berisi di bawah ini:
   a. Penilaian terhadap kondisi teknologi informasi saat ini, kekuatan kelemahan, serta, tantangan dan ancaman saat ini.
   b. Tujuan atau arah jangka panjang, jasa informasi masa depan harus disediakan, strategi keseluruhan terhadap intra organisasi maupun interorganisasi.
   c. Strategi pengembangan, visi dibidang teknologi informasi, aplikasi masa depan, kebutuhan dana, pendekatan dan monotoring terhadap pelaksanaan strategi.
2. Operational Plan,
   Operational Plan (Rencana Jangka Pendek):
   a. Progress report berisi keterangan tentang keberhasilan dan kegagalan pencapaian rencana sekarang. Perubahaan yang besar terhadap platform hardware-software, hal-hal yang baru harus di lakukan.
   b. Initiatives to be undertaken, berisi keterangan tentang perkembangan sistem perubahaan hardware-soft ware, tambahan karyawan dan pengembangannya, penambahaan sumber daya keuangan.
   c. Implementation Scheduler, berisi keterangan tentang kapan mulai selesainya, setiap proyek utama, kejadian yang penting, prosedur control, proyek yang di terapkan.

4.5 Perencanaan Sistem

Rancangan sistem adalah penentuan proses dan data di perlukan oleh sistem baru, jika sistem itu berbasis komputer, rancangannya dapat menyertakan spesifikasi jenis peralatan yang digunakan. Perencanaan Sistem terdiri dari kegiatan- kegiatan desain untuk menghasilkan spesifikasi sistem yang dapat memenuhi kebutuhan fungsional yang dikembangkan ke dalam proses analis sistem.

Jadi dengan demikian perancangan sistem merupakan proses-proses atau aktivitas-aktivitas untuk menentukan atau menghasilkan speksifikasi system yang diperlukan oleh sistem baru yang memenuhi kebutuhan fungsional dengan tujuan untuk memberikan gambaran secara umum oleh pemakai pada sistem yang baru.

Menurut O'Brien (2005) perancangan sistem terdiri dari tiga aktivitas yaitu:

1. Desain User Interface, yaitu merancang layar, Formulir dan dialog
2. Desain Data yaitu menentukan entitiy (Objek), atribut, relationship, kaidah intregritas dan lain –lain
3. Desain Proses yaitu membuat program dan prosedur seperti user services, application services, dan data Services

Interaksi manusia dan komputer(Imk) merupakan disiplin ilmu yang mempelajari mengenai suatu hubungan diantara manusia dan komputer yang diantaranya itu meliputi perancangan, evaluasi, serta implementasi antarmuka pengguna komputer supaya dapat mudah digunakan oleh manusia. Sedangkan interaksi manusia dan komputer itu juga merupakan serangkaian proses, dialog serta kegiatan(aktivitas) yang dilakukan oleh manusia untuk dapat berinteraksi dengan komputer dengan secara interaktif untuk dapat melaksanakan serta menyelesaikan tugas yang diinginkan.

Menurut Shneiderman dan Plaisant (2010), Interaksi Manusia dan Komputer (IMK) adalah disiplin ilmu yang berhubungan dengan perancangan, evaluasi, dan implementasi sistem komputer interaktif untuk digunakan oleh manusia. Titik berat IMK adalah perancangan dan evaluasi antarmuka pemakai (user interface). Antarmuka pemakai adalah bagian sistem komputer yang memungkinkan manusia berinteraksi dengan komputer.

Menurut Pressman (2001) rekayasa Software adalah aplikasi dari pendekatan kuantifiabel, displin, dan sistematis pada pengembangan, operasi, dan pemeliharaan perangkat lunak, salah satu model rekayasa perangkat Lunak yang

di sebut Linear Sequential Model yang biasa disebut dengan Classic Life Cycle atau Waterfall Model.

Dalam model ini pendekatan pengembangan software di lakukan sistematik dan sequential yang di awali dengan System Enginering, Analysis, Design, Coding, Testing dan Maintanence.

4.6 Struktur Organisasi Fungsi Sistem Informasi

Secara umum sistem informasi di letakan pada fungsi depertemen sistem informasi, di dalam depertemen Ini berisi bagian pengembangan sistem. Bagian programming, bagian pengeoprasian, penyiapan data dan bagian Pendukung atau control.

Stuktur Organisasi pusat komputer secara Tradisional terdiri dari:

1. Bagian Aplikasi (terdiri dari para sistem analis dan Programmer)
2. Bagian Produksi (terdiri dari para Operator yang secara langsung menjalankan operasional computer
3. Bagian dukungan Teknis (terdiri dari para Spesialis Operating sistem, ahli Dalam control terhadap pemakai jasa sistem informasi, Top Manager harus menbuat policy dan Prosedur yang akan membuat user menggunakan jasa sistem informasi secara Efektif dan Efisien.

4.6.1 Pengendalian Manajemen Pengembangan Sistem

Pengendalian, pengembangan dan pemeliharaan sistem diperlukan untuk mencegah dan mendeteksi Kemungkinan kesalahan pada waktu pengembangan dan pemeliharaan sistem, serta untuk menperoleh keyakinan memadai bahwa sistem berbasis teknologi informasi di kembangkan dan di pelihara dengan cara efesien dan melalui proses otorisasi dengan semestinya.

Pengendalian pengembangan sistem adalah sebagai berikut:

1. Pengembang sistem harus melibatkan partisipasi pemakai, manajemen,auditor

2. Adanya standard dan pedoman maupun prosedur 3.Dilaksanakannya pengujian sistem dan konversi dengan cermat. 4.Penelaahan setelah pemasangan atau instalasi.

4.7 Interaksi Manusia dan Komputer

Dalam merancang suatu sistem harus di perlukan satu hal sangat pentng yaitu interaksi anatara user /pengguna dengan sistem. Interaksi ini haruslah user friendly, yang artinya mudah di gunakan oleh pengguna yang awan sekalipun. (Shneiderman,1998).

Dalam merancang suatu sistem interkasi manusia dengan dan komputer yang baik, maka ada delapan (8) aturan yang diperhatikan:

1. Konsisten dalam warna, tampilan, jenis huruf, perintah/ menu
2. Memungkinkan Frequent users menggunakan shortcuts, penggunaan shortcuts untuk memudahkan Pemakai saat berintraksi dengan komputer sehingga perintah dan fasilitas yang tersedia lebih mudah di mengerti dan lebih cepat di akses.
3. Memberikan umpan balik yang imformatif, setipa aksi pemakai sebaliknya ada umpan balik dari system dan umpan balik (respon) atau message di layar, harus di buat sederhana agar mudah di megerti untuk menetukan langkah selanjutnya.
4. Merancang dialog yang baik, dari awal sampai penutupan. urutan dari aksi sebaliknya di atur dengan baik yaitu dengan pembukaan, isi dan penutup.
5. Memberikan pencegahan dan penanganan kesalahan yang sederhana sebisa mungkin rancangan sistem di buat agar pemakai tidak menbuat kesalahan contohnya jika suatu kolom isian tidak di perbolehkan pengisian jenis alphabet , maka jika di isi alphabet layar harus segera menberikan error message.
6. Memungkinkan pembalikan aksi yang mudah, dalam merancang sistem sebaiknya aksi dapat dikembalikan. pengembalian aksi dapat berupa aksi tunggal, tugas entry atau kelompok yang lengkap.

7. Mendukung pusat kendali internal, pemakai dapat mengusai sistem, dan sistem merespon intruksi-Intruksi dari mereka.
8. Mengurangi beban ingatan dari jangka pendek, manusia memiliki keterbatasan dalam meningat memory singkat, tampilan halaman yang banyak menggabungkan frekuensi gerakan window sebaliknya dikurangi, buatlah tampilan sederhana, dengan menyediakan penyingkatan kode dan informasi lain.

4.8 Sistem Development Life Cycle Approach

System development life cycle approach adalah metode pengembahan sistem aplikasi yang terdiri dari beberapa tahap, setiap tahap mempunyai jenis kegiatan tertentu:

1. Feasibility Study
   Dengan kriteria cost benefit untuk mengusulkan aplikasi.
2. Information Analysis Menentukan keperluan user
3. Sistem Design,
   Mendesain user interface, file yang di gunakan dan fungsi proses informasi yang di lakukan oleh sistem.
4. Program Development
   Design, codding, compiling, testing, dan dokumentasi program
5. Procedures And From Development
   Desain dan dokumentasi prosedur sistem dan formulir yang di gunakan user pada sistem.
6. Acceptance Test
   Testing terakhir terhadap sistem dan persetujuan formal serta penerimaan oleh management dan user.
7. Conversion
   Konversi atau perubahan dari sistem lama ke sistem baru

8. Operation and maintance
   Penambahan sistem selama implementasi dan modifikasi serta maintances bila di ketahui ada masalah

Bab 5

Sistem berbasis Teknologi Informasi

5.1 Sistem berbasis Teknologi Informasi

Di dalam suatu sistem berbasis teknologi informasi, pengendalian sumber data yang baik adalah:

1. User harus dapat berbagi data
2. Data harus tersedia di gunakan kapan saja, di mana pun, dan dalam bentuk apa pun.
3. Sistem manajemen data harus menjamin adanya sistem penyimpanan yang efisien tidak terjadi redundancy data, adanya data security
4. data harus dapat di modifikasi dengan mudah.

Setiap organisasi tentu mengakui bahwa data merupakan sumber daya yang kritis dan harus di kelolah dengan baik, karena itu kita mencari cara untuk menangani sistem manajemen data. Solusi teknis adalah dengan database management sistem (DBMS) dan data repository system (DRS), selain itu di perkenalkan dua keahlian penting yaitu data administration (DA) dan database administrator (DBA)

5.2 Tugas data Adiministration (DA) dan database administrator (DBA)

Database administrator adalah orang yang bertugas untuk menyimpan dan mengelola data perusahaan dengan menggunakan jenis perangkat lunak khusus. Data yang dimaksud dapat mencakup berbagai informasi seperti data finansial, informasi sensus, akun pengguna. Seorang database administrator atau DBA akan memastikan bahwa data-data yang ada dalam perusahaan tadi tersedia, tersimpan dengan baik dan aman agar tidak hilang atau diakses oleh orang-orang yang tidak memiliki kepentingan.

Seorang data administrator memiliki peran dan tugas yang beragam di dalam perusahaan. Beberapa tanggung jawab dan tugas database administrator adalah:

1. Mengevaluasi pembelian software database
2. Melakukan pengawasan terhadap modifikasi dari software database yang ada untuk memenuhi kebutuhan employer
3. Menjaga integritas dan kinerja basis data perusahaan
4. Menjamin bahwa data disimpan dengan aman dan optimal
5. Memberi tahu end user tentang perubahan dalam database dan melatih mereka cara untuk memanfaatkan sistem
6. Membuat user accounts baru dan perizinan
7. Menguji modifikasi pada struktur database
8. Mengoptimalkan sistem database dengan menginstal pembaruan secara teratur
9. Memperbarui program anti virus di server database secara teratur
10. Mendiagnosis masalah yang ada pada sistem database dan memecahkan masalah tersebut
11. Menggabungkan database lama
12. Melakukan perencanaan kapasitas
13. Memantau perangkat keras dan sistem operasi server database
14. Membuat back up dan memulihkannya untuk mencegah kehilangan data

5.2.1 Jenis-Jenis Database Administrator

Ada jenis database administrator serba guna yang melakukan semua jenis pekerjaan yang terkait dengan administrasi data. Yaitu:

1. System database administrator.
   Bertanggung jawab atas aspek fisik dan teknis dari database seperti menginstal upgrade dan patch untuk memperbaiki bug program. Biasanya jenis database administrator ini memiliki latar belakang dalam arsitektur sistem dan bertugas memastikan bahwa database di sistem komputer berfungsi dengan baik.
2. Application database administrator.
   Fokus mendukung database yang telah dirancang untuk aplikasi atau serangkaian aplikasi tertentu seperti software customer service.

5.2.2 Pemahaman yang Baik Terhadap Tugas DA dan DBA

Pemahaman yang baik terhadap tugas DBA dan DBA sebagai berikut:

1. Jika DA dan DBA tidak bekerja baik, maka keamanan harta, keutuhan data efektivitas dan efesiensi system pada lingkungan database dapat rusak berat. DA dan DBA, merupakan sumber daya yang penting untuk memberikan informasi tentang kekuatan dan kelemahan lingkungan database, karena mereka merupakan pusat kmunikasi antara pemakai dan database
2. Fungsi pengeloaan sumberdaya data dilakukan oleh Data Administrator (DA) dan Database Administrator (DBA). Kedua administrator ini melakukan fungsi pendefinisian data, pencatatan data, perbaikan data, penghapusan data, penyajian data, pendidikan dan pelayanan pemakai, pengamanan data, dan memonitor penggunaan data. Antara DA dan DBA memeran tugas yang berbeda dalam menjalankan fungsi tersebut.
3. Definiting (pendefinisian) data
   Fungsi DA yaitu menentukan kebutuhan pengguna guna menetapkan definisi skema eksternal dan konseptual. Sedangkan fungs DBA yaitu menentukan definisi skema internal yang lebih banyak berhubungan dengan programer.

4. Creating (pencatatan) data
   Fungsi DA adalah memberitahukan pengguna tentang prosedur pengumpulan data, cara memeriksa, dan validasi. Sedangkan fungsi DBA adalah menyiapkan program untuk membuat data.
5. Redefining / restructuring (perbaikan) data
   Fungsi DA adalah menetapkan definisi baru skema konseptual, skema eksternal dan membuat pengguna nyaman dengan konsep baru tersebut. Sedangkan fungsi DBA adalah menetapkan definisi skema internal yang baru, megubah database agar sesuai dengan definisi skema yang baru.
6. Retiring (pebuangan) data
   Fungsi DA adalah menetapkan kebijakan retiring data atau membuang data yang tidak diperlukan. Sedangkan fungsi DBA adalah melakukan kebijakan retirement atau memisahkan data yang sudah tidak digunakan lagi.
7. Making database available to users (penyajian data)
   Fungsi DA adalah menentukan peralatan yang dibutuhkan user, menguji dan mengevaluasi peralatan tersebut. Sedangkan fungsi DBA adalah menentukan peralatan yang dibutuhkan programmer, menguji dan mengevaluasi peralatan tersebut.
8. Informing and servicing users (Pelatihan dan pelayanan pemakai).
   Fngsi DA adalah menjawab pertanyaan user dan mendidik user, menyampaikan informasi tentang kebijakan dan menyediakan informasi tentang skema konseptual dan skema eksternal. Sedangkan fungsi DBA adalah menjawab pertanyaan programmer dan mendidiknya, menyiapkan skema internal.
9. Maintaining database integrity (Memelihara dan menganankan data).
   Fungsi DA adalah mengembangkan dan mengumumkan standar mutu organisasi, membantu pengguna untuk merumuskan aplikasi. Sedangkan fungsi DBA adalah melakukan pengendalian database, membantu programmer untuk merancang dan emngimplementasikan kontrol aplikasi.

10. Monitoring operations (memonitor pemakain data). Fungsi DA adalah mengawasi aktivitas pengguna dalam pemakaian database. Sedangkan fungsi DBA adalah mengawasi aktivitas programmer dalam pemakaian database, mengumpulkan tenaga kerja dan memperbaiki database.

Penyimpangan oleh DA dan DBA:
1. Ketidak kompetenan dalam menjalankan peran DA dan DBA, adanya risiko DA dan DBA tidak mampu menjalankan perannya, jadi auditor harus memastikan adanya pengendalian manajemen.
2. DA dan DBA mempunyai peluang untuk melakukan penyelewengan karena DA dan DBA mempunyai kekuasaan dalam fungsi komunikasi dan koordinasi pada lingkungan database.
3. Adanya alat yang dapat digunakan untuk mengabaikan kontrol

Cara mengatasi exposure DA dan DBA:
1. Menempatkan jabatan DA dan DBA dengan tepat
2. Perlu adanya pelatihan bagi DA dan DBA
3. Adanya pemisahan tugas yang jelas bagi DA dan DBA

5.3 Definisi Database

Pada sistem database ada tiga tipe pendefinisian yang harus di lakukan yaitu:
1. External schema, sebuah schema eksternal menperlihatkan keterangan tentang pandangan pemakai terhadap database sebagai suatu objek/ entity, attribute dari objek/ entity, data integrity costains pada objek / entity yang di minta oleh pemakai, karena banyak pemakai maka eksternal skema ini juga banyak
2. Conceptual schema: skema ini memperlihatkan database dari perspektif users, Isi skema konsep adalah semua objek / entity yang ada pada database, semua attribute, semua hubungan antara objek/entity dan semua integrity constraint pada objek / entity
3. Internal Schema: skema ini menunjukkan peta database (Map) ke fisik media penyimpanan, Hal ini berisi records, fields.access paths, dan

proses yang di gunakan untuk menggambarkan objek / entity, attribute objek relasi/ hubungan antara objek/entity seperti yang di cantumkan pada skema konseptual.

5.4 Database Intergrity

Integritas data (Everest,1986) mengidentifikasi ke dalam 6 hal yang harus di lakukan oleh DA dan DBA untuk Mengontrol aktivitas mereka, yaitu:

1. Definition Control: DA dan DBA menetapkan control untuk memastikan bahwa database selalu sesuai dengan definisinya,DA mengembangkan dan menyebar luaskan standar definisi data yang telah di buat dan melakukan pengawasan terhadap pencapaian standar tersebut.
2. Existence control: DA dan DBA melakukan pengamanan terhadap database yang ada dengan melakukan backup dan recovery yang di perlukan.
3. Access control: control akses, seperti password, mencegah kelalaian atau memperlihatkan data yang tidak seharusnya pada database.. berbagai akses level control di perlukan untuk jenis data. group jenis data, dan file, untuk mencegah hal yang tidak sama, pemisahan fungsi harus di lakukan agar orang yang memiliki akses control pada semua level tidak sama.
4. Update control: membatasi pengubahaan database hanya oleh user database yang sah saja. Otorisasi update terdiri dari dua hal: penambahaan database pada database dan wewenang untuk mengubah dan menghapus data yang ada.
5. Concurrency control (pemakaian simultan), integritas data dapat bermasalah, bila satu data yang sama di akses oleh dua proses dalam waktu yang bersamaan, jika akses bersama-sama tidak di atur, database dapat menjadi error
6. Quality control: control kwalitas bertugas untuk memastikan keakuratan data, kelengkapan, dan konsisitensi data yang maintance pada database.

7. Auditor harus melakukan wawancara dengan DA dan DBA untuk mengetahui bagaimana control yang Mereka lakukan untuk mengawasi keutuhan database. auditor juga harus mewawancara pemakai database Untuk menentukan level peringatan terhadap control itu.

Strategi Implementasi pengintegrasian Tiga strategi utama dari implementasi dan integrasi modul adalah sebagai berikut:

1. Top-Down, strategi ini digunakan jika, modul level atas (high-level modules) dibuat (coding), di test, dan diintegrasikan sebelum modul level bawah (low-level modules). Keuntungannya adalah kesalahan pada modul level atas dapat teridentifikasi lebih dini, kerugiannya adalah pada saat uji coba program akan menemui kesulitan ketika modul level bawah menemukan kesalahan fungsi input- output yang sangat sulit.
2. Bottom up, strategi ini digunakan jika, modul level bawah di buat (coding), di test dan diintegrasikan sebelum modul level atas di buat. Keuntungannya adalah modul level rendah yang merupakan operasi yang paling sulit di implementasikan dan diuji terlebih dahulu. Kerugiannya adalah pendekatan ini sangat sulit untuk di teliti seluruh operasinya, sebelum programnya selesai dibuat.
3. Threads, strategi ini digunakan jika, keputusan dibuat terlebih dahulu untuk fungsi program yang akan dibuat, kemudian modul yang akan mendukungnya baru dibuat dan kemudian diimplementasikan untuk menghasilkan fungsi yang penting. Keuntungannya adalah fungsi yang paling penting di implementasikan terlebih dahulu. Kerugiannya adalah integrasi dari modul yang berikutnya mungkin akan lebih sulit, jika dibandingkan dengan pendekatan top-down atau bottom-up.

Auditor perlu mencari bukti bahwa strategi yang dipilih manajemen adalah tepat khususnya pada program yang besar, penggunaan strategi yang salah dapat mengakibatkan program yang dihasilkan menjadi kurang berkualitas. Auditor dapat melakukan wawancara untuk menguji apakah manajemen menggunakan pendekatan sistematik untuk memilih strategi implementas dan integrasi.

Mereka juga dapat menguji dokumentasi program untuk memperoleh bukti tipe strategi yang telah di pilih. Untuk memonitor agar pelaksanaan tidak bertentangan dengan rencana awal, beberapa teknik dapat digunakan seperti:

1. Work Breakdown Structures (WBS), dengan teknik ini kita dapat mengidentifikasi tugas-tugas yang spesifik untuk pengembangan, pengadaan, dan implementasi software yang dibutuhkan.
2. Gantt Chart, dapat digunakan untuk membantu mengatur tugas. Teknik ini akan menunjukan kapan tugas harus dimulai dan diselesaikan, tugas apa yang
3. harus dibuat bersama-sama, dan tugas apa yang harus dihasilkan secara serial, serta membantu mengidentifikasi konsekuensi dari keterlambatan penyelesaian tugas tersebut. Kemajuan dari sebuah software dapat di plot pada gantt charts untuk menunjukkan apakah proyek telah berjalan dengan seharusnya.
4. Program Evaluation and review technique (PERT), menunjukan tugas-tugas yang harus diselesaikan, bagaimana hubungannya, kebutuhan sumber daya apa untuk setiap tugas-tugasnya. Evaluasi program dan tinjauan teknis (PERT) charts menunjukkan tugas yang harus dilakukan, keterkaitan dan kebutuhan sumber daya untuk setiap tugas. PERT charts membiarkan masalah sepanjang keterlambatan dalam penyelesaian tugas yang tertunda akan menghasilkan software secara keseluruhan. PERT charts juga memungkinkan manajemen untuk menentukan konsekuensi penyelesaian awal atau akhir tugas.

Tanggung Jawab DBA adalah menangani Struktur basis data adalah:

1. Merancang skema
   DBA biasanya tidak terlibat dalam perancangan basisdata mulai dari awal. Oleh karena itu, setiap terjadi perubahan struktur basis data yang berpengaruh pada skema / relasi antar tabel harus selalu dicatat
2. Mengawasi terjadinya redundancy
   Redundancy dapat terjadi pada dua hal, yaitu performance dan data integrity. DBA harus menetapkan prosedur tertentu untuk melakukan rekonsiliasi data untuk menghindari terjadinya redundancy

3. Melakukan pengawasan konfigurasi permintaan atas perubahan struktur basisdata
   DBA bertugas menyusun laporan secara berkala mengenai pemakai yang aktif, serta file dan data yang dipakai, dan metode akses yang digunakan. Disamping itu juga dicatat terjadinya kesalahan. Hal tersebut diperlukan untuk menentukan apakah diperlukan adanya perubahan struktur basisdata demi peningkatan performance
4. Menjadwalkan dan mengadakan pertemuan apabila terjadi perubahan struktur basisdata
5. Menerapkan perubahan skema
   Perubahan harus dilakukan pada basisdata ujicoba, agar pemakai dapat mengujinya sebelum diterapkan pada sistem yang sesungguhnya
6. Merawat dokumentasi pemakai
   Merawat dokumentasi DBA – untuk memperoleh informasi tentang perubahan yang telah dilakukan, bagaimana dan kapan dilakukanManajemen DBMS

5.5 Konsep dan kontrol dan Audit Software

Audit Software adalah software yang digunakan oleh auditor untuk membantu tugas auditnya terutama untuk menguji keandalan sistem dan integritas data.

Software audit ini beraneka ragam, dan sebagian besar tersedia secara luas dalam bentuk paket jadi. Berikut ini akan dibahas beberapa jenis audit software:

1. Generalized Audit Software (GAS)
   Merupakan audit yang digunakan untuk hampir seluruh pekerjaan audit.. Misal: ACL (audit common language). GAS memiliki kemampuan fungsional sbb:
   a. Untuk akses file
   b. Untuk menyusun ulang file
   c. Untuk seleksi(mengambil data yang diinginkan)
   d. Untuk statistik

e. Untuk aritmatik, penambahan, pengurangan dan pembagian
f. Untuk analisi pengelompokkan data dan frekuensi
g. Untuk membuat file baru dan up-date data
h. Untuk pelaporan

Pekerjaan audit yang dapat dilakukan dengan GAS adalah:

a. Memeriksa mutu data, auditor dapat menggunakan GAS untuk menguji eksistensi, keakuratan, kelengkapan, konsistensi dan jangka waktu pemeliharaan data dan tempat penyimpanan.
b. Memeriksa kualitas dari proses sistem, Auditor dapat menggunakan teknik paralel simulation
c. Memeriksa eksistensi/ keberadaan aset yang diwakili oleh data klien
d. Melakukan analisis analitik, membandingkan angka dalam laporan keuangan dengan angka yang lain atau dari catatan klien

Keterbatasan GAS:

a. Hanya dapat digunakan untuk ex-post audit/ audit untuk transaksi yang sudah terjadi, tidak bisa melakukan audit pada saat terjadi transaksi (concurrent audit).
b. Kemampuan terbatas dalam menguji mutu dari prose pengolaan data dari klien.
c. Kemampuan terbatas dalam menemukan kemungkinan terjadi kesalahan atau kegagalan pada sistem.

Cara GAS untuk mengakses data klien. Ada berbagai cara auditor dapat mengakses data auditan dengan menggunakan GAS:

a. Data di copy ke disk
b. Melalui modem
c. Melalui LAN klien

2. Industry Spesifik Audit software (ISAS)

Merupakan software audit yang di buat khusus berdasarkan jenis industri yang akan diaudit. Perbedaan utama ISAS dengan GAS

a. IASA dapat dikembangkan untuk mengakses data spesifik yang digunakan secara luas dalam industri.

b. ISAS di implementasikan kepada industri tertentu yang menyediakan perintah high- level yang memuat fungsi audit umum yang dibutuhkan untuk mengaudit industri tersebut.

3. High- Level Language (4GL)
   Memiliki fungsi yang sama dengan GAS dalam audit, contoh adalah Fourth generation languages seperti SQL, QBE, SPSS dan SAS.
   Alasan penggunaan Fourth- generation languages
   a. Fungsi yang terdapat pada GAS yang ada pada 4GL.
   b. Auditor lebih menguasai 4GL dapat digunakan lebih mudah di banding GAS
   c. 4GL digunakan secara luas dalam organisasi yang akan membantu auditor dalam pekerjaan
4. Utility software
   Software untuk berbagai keperluan umum yang tidak hanya diperlukan oleh auditor. Jenis-jenis kegunaan utility audit software
   a. Untuk keamanan Integritas
   b. Untuk menguji mutu dari data,
   c. Untuk mengamani sistem klien
   d. Untuk memeriksa utility
   e. Untuk mengukur efisiensi operasi Auditor menggunakan utility software dengan alasan:
      - Dapat digunakan untuk melakukan keamanan khusus atau fungsi yang berhubungan dengan integritas.
      - Dapat digunakan untuk mendownlod data
      - Dapat melaksanakan fungsi yang tidak dapat dilakukan oleh GAS atau software audit lainnya.
      - Dapat menyelesaikan tugas audit dengan cara efektif dan efisien dibanding software audit.
      - Dapat digunakan auditor untuk membantu mengembangkan software audit baru.
5. Expert System Software (ES)
   Merupakan program yang di buat berdasarkan keahlian manusia yang mempunyai kemampuan untuk menggantikan tenaga ahli tersebut

pada saat terjadi masalah. Alasan auditor mengembangkan, memelihara dan menggunakan ES:

a. ES menyediakan penetahuan yang hanya di miliki sebagian kecil auditor.
b. Karena perkembangan teknologi yang pesat, sulit bagi auditor untuk menguasai pengetahuan yang mungkin atau dihadapkan dalam fungsi audit.

6. Special Audit Software

Merupakan software audit khusus untuk pelaksanaan pekerjaan audit tertentu.

Alasan menggunakan special audit software

a. Tidak tersedianya software alternatif
b. Keterbatasan fungsi dari software alternatif
c. Pertimbangan efisiensi
d. Meningkatkan pemahaman tentang sistem
e. Kesempatan untuk implementasi yang mudah
f. Peningkatan kemandirian auditor

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.

Journal of Computer Science and Network Security, VOL.10 No.6, June 2010. Surabaya: ITS Press.

Tanuwijaya, H. dan Sarno, R. 2010. Comparation of Cobit Maturity Model and Structural Equation Model for Measuring the Alignment between University Academic Regulati ons and Information Technology Goals, International

Webber, R. 1999. Information System Control and Audit, The University ofQueensland, Prentice Hall

Yuwono, S. 2006. Petunjuk Praktis Penyusunan Balanced Scorecard. Jakarta: Gramedia Pustaka Utama

Biodata Penulis

Silvia Ratna, Lahir di Puruk-Cahu Provinsi Kalimantan-Tengah pada tanggal 13 September 1975, Sekolah dasar sampai dengan SMA ditamatkan di Puruk-Cahu. Pada Tahun 1995 melanjutkan kuliah di STMIK AKAKOM Yogyakarta dan memperoleh gelar Sarjana Komputer (S.Kom) pada tahun 2000, Pada tahun 2006 melanjutkan pendidikan S2 di STTS Surabaya dan memperoleh gelar Magister Komputer (M.Kom) pada tahun 2008, selanjutnya pada tahun 2011 melanjutkan pendidikan S3 Program Doktor Ilmu Administrasi Minat Ilmu Administrasi Bisnis di Fakultas Ilmu Administrasi Universitas Brawijaya Malang dan selesai pada tahun 2016 dengan menyandang gelar Doktor (Dr.), Pengalaman kerja Menjadi Dosen dan Pembantu Ketua 1 pada STMIK Banjarbaru(Kampus Banjarmasin) pada tahun 2003 s/d 2005, tahun 2005 diterima menjadi Dosen PNS Kopertis Wilayah XI dpk pada Universitas Islam Kalimantan Muhammad Arsyad Al-Banjari, tahun 2008 s/d 2011 menjabat sebagai Pembantu Dekan II pada Fakultas Teknik Universitas Islam Kalimantan Muhammad Arsyad Al-Banjari (UNISKA MAAB) dan pada tahun 2011 sd 2013 menjabat sebagai Dekan pada Fakultas Teknik Universitas Islam Kalimantan Muhammad Arsyad Al-Banjari, Tahun 2014 s/d Sekarang menjabat sebagai Dekan pada Fakultas Teknologi Informasi Universitas Islam Kalimantan Muhammad Arsyad Al-Banjari, sebagai Asesor BKD dan sebagai pengurus sekaligus penyantun di Yayasan Graha Education yang menaungi Pendidikan Anak Usia Dini Islam Terpadu “Anak sholeh Mandiri” (PAUD IT ASM), SD IT ASM, SMP IT ASM

Audit 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.

Buku ini membahas:

YAYASAN KITA MENULIS
press@kitamenulis.id
www.kitamenulis.id

ISBN 978-623-342-860-6