

BAB II

LANDASAN TEORI

2.1 Audit

2.1.1 Pengertian Audit

Menurut Arens, Elder, & Beasley (2012), *“Auditing is the accumulation and evaluation of evidence about information to determine and report on the degree of correspondence between the information and established criteria. Auditing should be done by a competent, independent person”*, yang berarti audit merupakan akumulasi dan evaluasi bukti mengenai informasi yang menentukan dan melaporkan derajat kesesuaian antara informasi dan kriteria yang ditetapkan. Audit harus dilakukan oleh orang yang berwenang, bebas atau tidak terikat.

Sedangkan menurut Gramling, Johnstone, & Rittenberg (2012), *“Systematic process of objectively obtaining and evaluating evidence regarding assertions about economic actions and events to ascertain the degree of correspondence between those assertions and established criteria and communicating the result to interested users”*, yang berarti audit merupakan proses sistematis yang secara objektif mendapatkan dan mengevaluasi bukti mengenai pernyataan tentang tindakan dan peristiwa ekonomi untuk memastikan tingkat korespondensi antara pernyataan dan kriteria yang ditetapkan dan mengkomunikasikan hasilnya kepada para pengguna yang tertarik.

Dari kedua pengertian tersebut dapat disimpulkan bahwa audit merupakan proses akumulasi yang secara objektif mendapatkan dan mengevaluasi bukti mengenai informasi atau pernyataan tentang tindakan dan peristiwa ekonomi untuk menentukan dan melaporkan derajat kesesuaian antara informasi dan kriteria yang telah ditetapkan dan mengkomunikasikan hasil dari audit tersebut yang dilakukan oleh orang yang berwenang, bebas dan tidak terikat kepada para pengguna.

2.1.2 Jenis Audit

Berdasarkan UU No.15 tahun 2004, terdapat tiga jenis audit menurut tujuan pelaksanaan audit, yaitu:

1. Audit Keuangan

Audit keuangan adalah untuk menentukan apakah informasi keuangan telah akurat dan dapat diandalkan (Sesuai Standar Akuntansi Pemerintah/SAP), serta untuk memberikan opini kewajaran atas penyajian laporan keuangan.

2. Audit Kinerja

Audit kinerja adalah pemeriksaan atas pengelolaan keuangan negara yang terdiri atas pemeriksaan aspek ekonomi dan efisiensi serta pemeriksaan aspek efektivitas. Dalam melakukan audit kinerja, auditor juga menguji kepatuhan terhadap ketentuan perundang-undangan serta pengendalian intern. Audit kinerja menghasilkan temuan, simpulan, dan rekomendasi.

Menentukan keandalan informasi kinerja, tingkat ketaatan, pemenuhan standar mutu operasi, efisiensi, ekonomis, dan efektivitas.

3. Audit Dengan Tujuan Tertentu

Audit dengan tujuan tertentu adalah pemeriksaan yang tidak termasuk dalam pemeriksaan keuangan dan pemeriksaan kinerja/audit operasional.

Sesuai dengan definisinya, jenis audit ini dapat berupa semua jenis audit, selain audit keuangan dan audit operasional. Jenis audit ini termasuk diantaranya audit ketaatan dan audit investigatif. Audit ketaatan bertujuan untuk menentukan apakah peraturan ekstern serta kebijakan dan prosedur intern telah dipenuhi, sedangkan audit investigative bertujuan untuk menentukan apakah kecurangan/peyimbangan benar terjadi.

2.1.3 Jenis Auditor

Jenis-jenis auditor dibagi menjadi 3 (tiga) jenis yang dapat dijelaskan sebagai berikut:

1. Auditor Indenpenden

Auditor indenpenden adalah auditor profesional yang menyediakan jasanya kepada masyarakat umum, terutama dalam bidang audit atas laporan keuangan yang dibuat oleh kliennya. Audit ini ditujukan untuk memenuhi kebutuhan para pemakai informasi keuangan, misalnya: kreditur, investor, instansi pemerintah (terutama instansi pajak). Untuk berpraktik sebagai auditor indenpenden, seseorang harus memenuhi persyaratan pendidikan dan pengalaman kerja tertentu. Auditor

independen harus telah lulus dari jurusan akuntansi fakultas ekonomi atau memiliki ijazah yang disamakan, telah mendapat gelar akuntan dari panitia ahli pertimbangan persamaan ijazah akuntan, lulus Ujian Sertifikasi Akuntan Publik (USAP), serta mendapatkan ijin praktek dari menteri keuangan.

2. Auditor Pemerintah

Auditor pemerintah adalah auditor profesional yang bekerja di instansi pemerintah yang tugas pokoknya melakukan audit atas pertanggungjawaban keuangan yang disajikan oleh unit-unit organisasi atau entitas pemerintah atau pertanggungjawaban keuangan yang ditujukan pemerintah.

3. Auditor Intern

Auditor intern adalah auditor yang bekerja dalam perusahaan (perusahaan negara atau perusahaan swasta). Tipe auditor ini dilibatkan dalam suatu aktivitas penilaian yang independen, disebut *internal auditing*.

Tugas pokok dari auditor intern ini adalah untuk menentukan apakah kebijakan dan prosedur yang ditetapkan oleh manajemen puncak telah dipatuhi, menentukan baik atau tidaknya penjagaan terhadap kekayaan organisasi, menentukan efisiensi dan efektivitas prosedur kegiatan organisasi, serta menentukan keandalan informasi yang dihasilkan oleh berbagai bagian organisasi.

2.1.4 Proses Audit

Proses audit adalah suatu metodologi yang tersusun baik untuk mengorganisasikan suatu audit untuk memastikan bahwa bukti-bukti yang terkumpul telah memadai dan kompeten serta semua tujuan audit yang tepat telah terspesifikasi dan dipenuhi. Menurut Arens, Elder & Beasley (2003;226-228) ada 4 (empat) tahap proses audit, yaitu:

1. Merencanakan dan mendesain pendekatan audit

Ada 2 (dua) pertimbangan utama yang mempengaruhi jenis pendekatan yang akan digunakan oleh auditor yaitu: harus terkumpulnya bukti audit yang cukup kompeten agar dapat memenuhi tanggung jawab profesional auditor dan biaya pengumpulan bukti audit ini haruslah seminimal mungkin.

Perencanaan dan perancangan suatu pendekatan audit terdiri dari 2 (dua) bagian yaitu, memperoleh pemahaman akan strategi bisnis klien dan memproses serta menilai resiko, dan memahami pengendalian intern dan menilai resiko pengendalian.

2. Melaksanakan uji pengendalian dan uji substantif dan transaksi

Ketika auditor telah mengurangi taksiran resiko pengendalian dengan mendasarkan diri pada pengidentifikasi pengendalian, ia selanjutnya dapat mengurangi lingkup audit pada sejumlah tempat dimana akurasi informasi dalam laporan keuangan yang terkait langsung dengan berbagai pengendalian tersebut harus didukung oleh pengumpulan berbagai bukti audit.

Auditor juga harus melakukan evaluasi atas pencatatan berbagai transaksi yang dilakukan oleh klien dengan menverifikasi nilai moneter dari berbagai transaksi itu.

3. Melaksanakan prosedur analitis dan uji rincian saldo

Terdapat dua kategori umum dari berbagai prosedur pada fase ini, yaitu: prosedur analitis dan uji rincian saldo. Prosedur analitis menggunakan perbandingan-perbandingan serta sebagai hubungan untuk menilai apakah saldo akun-akun atau data-data lainnya tampak wajar. Sedangkan uji rincian saldo merupakan berbagai prosedur spesifik yang ditujukan untuk menguji salah saji secara moneter pada akun-akun laporan keuangan.

4. Melengkapi proses audit dan menerbitkan suatu laporan audit

Setelah auditor melengkapi semua prosedur bagi setiap tujuan audit dan bagi setiap akun dalam laporan keuangan, merupakan hal yang penting untuk menggabungkan semua informasi yang diperoleh untuk mencapai suatu kesimpulan menyeluruh tentang apakah suatu laporan keuangan itu telah disajikan secara wajar

2.2 Jaringan Komputer

2.2.1 Sejarah Jaringan Komputer

Sejarah jaringan komputer bermula dari lahirnya konsep jaringan komputer pada tahun 1940-an di Amerika yang digagas oleh sebuah proyek pengembangan komputer MODEL I di laboratorium Bell dan group riset Universitas Harvard yang dipimpin profesor Howard Aiken. Pada mulanya proyek

tersebut hanyalah ingin memanfaatkan sebuah perangkat komputer yang harus dipakai bersama. Untuk mengerjakan beberapa proses tanpa banyak membuang waktu kosong dibuatlah proses beruntun (*Batch Processing*), sehingga beberapa program bisa dijalankan dalam sebuah komputer dengan kaidah antrian.

Kemudian pada tahun 1950-an ketika jenis komputer mulai berkembang sampai terciptanya super komputer, maka sebuah komputer harus melayani beberapa tempat yang tersedia (*terminal*), untuk itu ditemukan konsep distribusi proses berdasarkan waktu yang dikenal dengan nama TSS (*Time Sharing System*).

Maka untuk pertama kalinya bentuk jaringan (*network*) komputer diaplikasikan.

Pada sistem TSS beberapa terminal terhubung secara seri ke sebuah komputer atau perangkat lainnya yang terhubung dalam suatu jaringan (*host*) komputer.

Dalam proses TSS mulai terlihat perpaduan teknologi komputer dan teknologi telekomunikasi yang pada awalnya berkembang sendiri-sendiri. Departemen

Pertahanan Amerika, *U.S. Defense Advanced Research Projects Agency* (DARPA) memutuskan untuk mengadakan riset yang bertujuan untuk

menghubungkan sejumlah komputer sehingga membentuk jaringan organik pada tahun 1969. Program riset ini dikenal dengan nama ARPANET.[5] Pada tahun

1970, sudah lebih dari 10 komputer yang berhasil dihubungkan satu sama lain sehingga mereka bisa saling berkomunikasi dan membentuk sebuah jaringan. Dan

pada tahun 1970 itu juga setelah beban pekerjaan bertambah banyak dan harga perangkat komputer besar mulai terasa sangat mahal, maka mulailah digunakan

konsep proses distribusi (*Distributed Processing*). Dalam proses ini beberapa host komputer mengerjakan sebuah pekerjaan besar secara paralel untuk melayani

beberapa terminal yang tersambung secara seri disetiap host komputer. Dalam proses distribusi sudah mutlak diperlukan perpaduan yang mendalam antara teknologi komputer dan telekomunikasi, karena selain proses yang harus didistribusikan, semua host komputer wajib melayani terminal-terminalnya dalam satu perintah dari komputer pusat.

Pada tahun 1972, Roy Tomlinson berhasil menyempurnakan program surat elektronik (*email*) yang dibuatnya setahun yang lalu untuk ARPANET.

Program tersebut begitu mudah untuk digunakan, sehingga langsung menjadi populer. Pada tahun yang sama yaitu tahun 1972, ikon at (@) juga diperkenalkan sebagai lambang penting yang menunjukkan “at” atau “pada”. Tahun 1973, jaringan komputer ARPANET mulai dikembangkan meluas ke luar Amerika Serikat. Komputer University College di London merupakan komputer pertama yang ada di luar Amerika yang menjadi anggota jaringan Arpanet. Pada tahun yang sama yaitu tahun 1973, dua orang ahli komputer yakni Vinton Cerf dan Bob Kahn mempresentasikan sebuah gagasan yang lebih besar, yang menjadi cikal bakal pemikiran *International Network* (Internet). Ide ini dipresentasikan untuk pertama kalinya di Universitas Sussex. Hari bersejarah berikutnya adalah tanggal 26 Maret 1976, ketika Ratu Inggris berhasil mengirimkan surat elektronik dari Royal Signals and Radar Establishment di Malvern. Setahun kemudian, sudah lebih dari 100 komputer yang bergabung di ARPANET membentuk sebuah jaringan atau network.

Tom Truscott, Jim Ellis dan Steve Bellovin, menciptakan newsgroups pertama yang diberi nama USENET (User Network) pada tahun 1979. Tahun

1981, France Telecom menciptakan sesuatu hal yang baru dengan meluncurkan telepon televisi pertama, di mana orang bisa saling menelepon yang juga berhubungan dengan video link.

Seiring dengan bertambahnya komputer yang membentuk jaringan, dibutuhkan sebuah protokol resmi yang dapat diakui dan diterima oleh semua jaringan. Untuk itu, pada tahun 1982 dibentuk sebuah *Transmission Control Protocol* (TCP) atau lebih dikenal dengan sebutan *Internet Protocol* (IP) yang kita kenal hingga saat ini. Sementara itu, di Eropa muncul sebuah jaringan serupa yang dikenal dengan *Europe Network* (EUNET) yang meliputi wilayah Belanda, Inggris, Denmark, dan Swedia. Jaringan EUNET ini menyediakan jasa surat elektronik dan newsgroup USENET.

Untuk menyeragamkan alamat di jaringan komputer yang ada, maka pada tahun 1984 diperkenalkan Sistem Penamaan Domain atau domain name system, yang kini kita kenal dengan DNS. Komputer yang tersambung dengan jaringan yang ada sudah melebihi 1000 komputer lebih. Pada 1987, jumlah komputer yang tersambung ke jaringan melonjak 10 kali lipat menjadi 10000 lebih.

Jaringan komputer terus berkembang pada tahun 1988, Jarkko Oikarinen seorang berkebangsaan Finlandia menemukan sekaligus memperkenalkan Internet Relay Chat atau lebih dikenal dengan IRC yang memungkinkan dua orang atau lebih pengguna komputer dapat berinteraksi secara langsung dengan pengiriman pesan (*Chatting*). Akibatnya, setahun kemudian jumlah komputer yang saling berhubungan melonjak 10 kali lipat. tak kurang dari 100000 komputer

membentuk sebuah jaringan. Pertengahan tahun 1990 merupakan tahun yang paling bersejarah, ketika Tim Berners Lee merancang sebuah *programe* penyunting dan penjelajah yang dapat menjelajahi komputer yang satu dengan yang lainnya dengan membentuk jaringan. Programe inilah yang disebut Waring Wera Wanua atau *World Wide Web*.

Komputer yang saling tersambung membentuk jaringan sudah melampaui sejuta komputer pada tahun 1992. Dan pada tahun yang sama muncul istilah *surfing* (menjelajah). Dan pada tahun 1994, situs-situs di internet telah tumbuh menjadi 3000 alamat halaman, dan untuk pertama kalinya berbelanja melalui internet atau *virtual-shopping* atau *e-retail* muncul di situs. Pada tahun yang sama Yahoo! didirikan, yang juga sekaligus tahun kelahiran Netscape Navigator 1.0.

2.2.2 Pengertian Jaringan Komputer

Menurut Wajong, Andre M.R. (2012), jaringan komputer adalah sebuah kumpulan komputer, printer dan peralatan lainnya yang terhubung dalam satu kesatuan. Informasi dan data bergerak melalui kabel-kabel atau tanpa kabel sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen dan data, mencetak pada printer yang sama dan bersama-sama menggunakan hardware/software yang terhubung dengan jaringan. Setiap komputer, printer atau periferal yang terhubung dengan jaringan disebut node. Sebuah jaringan komputer dapat memiliki dua, puluhan, ribuan atau bahkan jutaan node.

Menurut Sofana (2011), jaringan komputer adalah suatu himpunan interkoneksi sejumlah komputer autonomus. Kata “autonomous” mengandung pengertian bahwa komputer tersebut memiliki kendali atas dirinya sendiri. Memiliki manajemen sendiri (ada admin sendiri), memiliki topologi jaringan, hardware dan software sendiri. Sedangkan, dua buah komputer dikatakan “interkoneksi” apabila keduanya berbagi resources yang dimiliki, seperti saling bertukar data/informasi, berbagi printer, berbagi media penyimpanan dan sebagainya.

Menurut S. Arlis (2010), jaringan komputer adalah himpunan antara 2 komputer atau lebih yang terhubung dengan media transmisi kabel atau tanpa kavel (*wireless*).

Dua unit komputer dikatakan terkoneksi apabila keduanya bisa saling bertukar data/informasi, berbagai *resource* yang dimiliki, seperti file, printer, media penyimpanan (*hardisk, floppy disk, cd-rom, flash disk, dll*). Data yang berupa teks, audio, maupun video bergerak melalui media kabel atau tanpa kabel sehingga memungkinkan pengguna komputer dalam jaringan komputer dapat saling bertukar *file/data*, mencetak pada printer yang sama dan menggunakan hardware/software yang terhubung dalam jaringan secara bersama-sama.

Sedangkan menurut Arens, Elder, & Beasley (2012), jaringan komputer adalah kumpulan beberapa komputer yang saling berhubungan dengan suatu teknologi. Dua komputer dapat dihubungkan melalui kawat tembaga (*copper wire*), *fiber optic, microwaves, infrared*, dan satelit komunikasi juga dapat

digunakan. *Internet* maupun *World Wide Web* (WWW) juga disebut jaringan komputer.

Dari pengertian diatas dapat disimpulkan bahwa jaringan komputer adalah sebuah sistem yang terdiri dari dua atau lebih komputer yang saling terhubung satu sama lain melalui media transmisi atau media komunikasi sehingga dapat saling komunikasi antara satu komputer dengan komputer lainnya, berbagi data, aplikasi maupun berbagi perangkat keras komputer.

2.2.3 Jenis Jaringan Komputer

Menurut Wajong, Andre M.R. (2012), secara umum jaringan komputer terbagi menjadi 5 (lima) jenis, yaitu:

1. *Local Area Network* (LAN)

LAN merupakan jaringan milik pribadi di dalam sebuah gedung atau kampus yang berukuran sampai beberapa kilometer. LAN sering kali digunakan untuk menghubungkan komputer-komputer pribadi dan *workstation* dalam kantor suatu perusahaan atau pabrik-pabrik untuk memakai bersama sumberdaya (misalnya printer) dan saling bertukar informasi.

2. *Metropolitan Area Nerwork* (MAN)

Pada dasarnya merupakan versi LAN yang berukuran lebih besar dan biasanya menggunakan teknologi yang sama dengan LAN. MAN dapat

mencakup kantor-kantor perusahaan yang letaknya berdekatan atau juga sebuah kota dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum. MAN mampu menunjang data dan suara, bahkan dapat berhubungan dengan jaringan televisi kabel.

3. *Wide Area Network (WAN)*

Jangkauannya mencakup daerah geografis yang luas, seringkali mencakup sebuah negara bahkan benua. WAN terdiri dari kumpulan mesin-mesin yang bertujuan untuk menjalankan program-program (aplikasi) pemakai.

4. *Internet*

Sebenarnya terdapat banyak jaringan di dunia ini, seringkali menggunakan perangkat keras dan perangkat lunak yang berbeda-beda. Orang yang terhubung ke jaringan sering berharap untuk bisa berkomunikasi dengan orang lain yang terhubung ke jaringan lainnya. Keinginan seperti ini memerlukan hubungan antar jaringan yang seringkali tidak kompatibel dan berbeda. Biasanya untuk melakukan hal ini diperlukan sebuah mesin yang disebut gateway guna melakukan hubungan dan melaksanakan terjemahan yang diperlukan, baik perangkat keras maupun perangkat lunaknya. Kumpulan jaringan yang terinterkoneksi inilah yang disebut dengan internet.

5. *Jaringan Tanpa Kabel*

Jaringan tanpa kabel merupakan suatu solusi terhadap komunikasi yang tidak bisa dilakukan dengan jaringan yang menggunakan kabel. Misalnya orang yang ingin mendapat informasi atau melakukan komunikasi

walaupun sedang berada diatas mobil atau pesawat terbang, maka mutlak jaringan tanpa kabel diperlukan karena koneksi kabel tidaklah mungkin dibuat di dalam mobil atau pesawat. Saat ini jaringan tanpa kabel sudah marak digunakan dengan memanfaatkan jasa satelit dan mampu memberikan kecepatan akses yang lebih cepat dibandingkan dengan jaringan yang menggunakan kabel.

2.3 IP Address

IP address adalah suatu alamat unik yang diberikan kepada sebuah komputer atau device lainnya yang merupakan sebuah identitas sehingga sebuah komputer atau device bisa menemukan device lain dalam sebuah jaringan. Pengenal yang unik sebenarnya sudah terdapat pada tiap-tiap komputer yang terhubung ke jaringan yaitu alamat yang terdapat pada kartu jaringan. Alamat ini tidak pernah sama kecuali terjadi “kecelakaan” dalam produksi kartu jaringan atau alamat tersebut diubah dengan sengaja.

IP address yang digunakan sebagai standar penggunaan dalam jaringan adalah *IP address* versi 4 (menggunakan format 32 bit), walaupun sekarang telah direlease *IP* versi 6 yang bertujuan untuk menanggulangi habisnya alamat yang bisa digunakan nantinya (H.V. Kimin, 2011)

Pembagian kelas-kelas *IP address* selalu didasarkan pada dua hal yaitu *network ID* dan *host ID* dari suatu *IP address* tertentu

2.3.1 Jenis-Jenis *IP Address*

Berdasarkan sifat dan fungsinya, alamat IP dalam sebuah jaringan computer dibagi menjadi beberapa jenis, yaitu IP publik, IP privat, IP statik, dan IP dinamis (Hasnul Arifin, 2010)

1. IP Publik

IP Publik merupakan alamat IP yang dikenal di *internet*, alamat IP ini telah ditetapkan oleh InterNIC dan berisi beberapa buah *network ID* yang telah dijamin unik (tidak mungkin ada yang sama).

2. IP Privat

IP Privat merupakan alamat yang hanya dikenal pada jaringan local. Alamat ini digunakan untuk *host-host* didalam sebuah jaringan yang tidak membutuhkan akses langsung ke *internet*.

3. IP Statik

IP Statik merupakan alamat IP yang diberikan/ditentukan secara manual (diisikan) oleh administrator/pengguna computer atau peralatan lain yang menggunakan protocol TCP/IP.

4. IP Dinamis

IP Dinamis merupakan alamat IP yang diberikan secara otomatis oleh sistem dari sebuah *server DHCP (Dynamic Host Configuration Protocol)* setiap kali komputer dihidupkan. IP dinamis biasanya diterapkan pada

jaringan dengan jumlah *host* yang banyak, sehingga memudahkan administrator jaringan dalam menerapkan alamat IP pada masing-masing *host*.

2.3.2 Pembagian IP Address

Setiap *IP address* selalu merupakan pasangan dari *network ID* yang digunakan untuk tempat dimana suatu komputer berada dan *host ID* yang digunakan untuk menunjukkan *workstation*, *server*, *router* dan semua *host* lainnya yang terdapat pada jaringan tersebut. Berikut adalah kelas-kelas IP yang bisa digunakan.

IP address dibagi menjadi kelas-kelas yakni kelas A, kelas B, kelas C, dan kelas D (S. Arlis, 2010).

1. *IP address* kelas A

IP address kelas A diberikan untuk jaringan dengan jumlah *host* yang sangat besar. Bit pertama dari *IP address* kelas A selalu diset 0 (nol) sehingga byte terdepan dari *IP address* kelas A selalu bernilai antara angka 0-127. Pada kelas ini, *network ID* (n) adalah 8 bit pertama sedangkan untuk *host ID* (h) adalah 24 bit berikutnya. *IP address* kelas A ini dapat menampung lebih kurang 16 juta *host*.

Karakteristik *IP Address* Kelas A

| | |
|----------------|---------------------------------------|
| Format | : 0nnnnnnn hhhhhhhh hhhhhhhh hhhhhhhh |
| Bit pertama | : 0 |
| Panjang NetwID | : 8 bit |

| | |
|----------------|---|
| Panjang HostID | : 24 bit |
| Byte pertama | : 0-127 |
| Jumlah | : 126 Kelas A (0 dan 127 dicadangkan) |
| Range IP | : 1.xxx.xxx.xxx sampai 126.xxx.xxx.xxx |
| Jumlah IP | : 16.777.214 IP address pada setiap kelas A |

2. *IP address* kelas B

IP address kelas B ini biasanya digunakan untuk jaringan yang berukuran sedang dan besar. Pada *IP address* kelas B ini 2 (dua) bit pertama dari IP selalu diset dengan 10 (satu nol) sehingga *byte* terdepan dari *IP address* kelas ini selalu bernilai 128 sampai 191.

Pada *IP address* kelas B ini, *network ID* adalah 16 bit pertama sedangkan untuk *host ID*nya adalah 16 bit berikutnya. *IP address* kelas B ini dapat menampung lebih kurang 65000 *host*. Berikut adalah karakteristik dari *IP address* kelas B.

Karakteristik *IP Address* Kelas B

| | |
|----------------|--|
| Format | : 10nnnnnn nnnnnnnn hhhhhhhh hhhhhhhh |
| Bit pertama | : 10 |
| Panjang NetwID | : 16 bit |
| Panjang HostID | : 16 bit |
| Byte pertama | : 128-191 |
| Jumlah | : 16.384 Kelas B |
| Range IP | : 128.0.xxx.xxx sampai 191.155.xxx.xxx |
| Jumlah IP | : 65.532 IP address pada setiap kelas B. |

3. *IP address* kelas C

IP address kelas C digunakan untuk jaringan yang lebih kecil seperti LAN. Pada *IP address* kelas C ini 3 (tiga) bit pertamanya selalu berisi 110 (satu satu nol). Bersama 21 bit berikutnya, angka ini membentuk *network ID* sebesar 24 bit dan 8 bit terakhir untuk *host ID*. Sebagai contoh jika *IP address* kelas C adalah 192.168.1.1 maka dapat dikatakan *network ID* dari IP tersebut adalah 192.168.1 dan *host ID* dari IP tersebut adalah 1.

IP address kelas C ini dapat menampung lebih kurang 2 juta *network* dengan masing-masing *network* memiliki 256 IP address. Berikut adalah karakteristik dari *IP address* kelas C.

Karakteristik *IP Address* Kelas C

| | |
|----------------|---------------------------------------|
| Format | : 110nnnnn nnnnnnnn nnnnnnnn hhhhhhhh |
| Bit pertama | : 110 |
| Panjang NetwID | : 24 bit |
| Panjang HostID | : 8 bit |
| Byte pertama | : 192-223 |
| Jumlah | : 8192 |
| Range IP | : 192.0.0.xxx sampai 223.255.255.xxx |
| Jumlah IP | : 254 IP address pada setiap kelas C |

2.4 *Sharing Folder*

Sharing Folder adalah suatu fasilitas yang memungkinkan setiap folder dapat di-sharing atau dibagi kepada komputer lain yang dalam jaringan yang sama dimana dapat diatur siapa saja yang boleh mengakses folder tersebut.

Manfaat sharing folder:

1. Memudahkan di dalam pengelolaan / management folder pada jaringan.
2. Dengan fasilitas ini kita tidak perlu men-copy suatu file atau folder dari suatu komputer kedalam media penyimpanan (flashdisk, hardisk external, dan cd) untuk selanjutnya kita buka di komputer lainnya.

Resiko sharing folder:

1. Mudah diserang virus.

IP Address diketahui orang lain yang bisa mengundang untuk di hack.\

2.5 *Open Systems Interconnection (OSI) Layer*

Open Systems Interconnection (OSI) adalah sebuah referensi model yang pertama kali muncul sebelum TCP/IP digunakan. Model ini diciptakan berdasarkan suatu proposal yang dibuat oleh International Standard Organization (ISO) sebagai awal langkah awal menuju standarisasi protocol internasional yang akan digunakan pada berbagai tingkatan layer nantinya (Andry Syahputra, 2002)

OSI Model ini terdiri dari 7 layer. Seperti gambar dibawah ini, masing-masing Layer menjelaskan fungsinya di sebuah jaringan.



Gambar 2.1 OSI Layer

2.5.1 Application Layer

OSI *Application* ini mengacu pada aplikasi yang melayani komunikasi.

Pada saat programmer membuat *software image editor*, mereka tidak perlu memikirkan untuk penambahan OSI Layer 7 ini. Karena Aplikasi tersebut tidak berhubungan dengan komputer yang lainnya. Lain halnya dengan pembuat program FTP. Mereka harus menambahkan kemampuan komunikasi pada *software* tersebut.

Pada Layer 7 kita akan sering menemukan Telnet, FTP, HTTP, SMTP atau SSH.

2.5.2 *Presentation Layer*

Tujuan dari layer ini adalah mendefinisikan format data yang mewakili data tersebut. Contoh format data adalah ASCII, JPEG, GIF, TIFF, MPEG. Mendefinisikan format data ini sangatlah penting. Contohnya sewaktu kita mengirim atau menerima *Email*. Yang biasanya dalam format ASCII atau HTML. Apabila formatnya tidak terdefiniskan dengan baik, tentu saja email itu tidak bisa di baca.

OSI *Layer 6* menyediakan layanan untuk *Layer* yang di atasnya. Dia memformat data yang akan dikirim melalui jaringan supaya aplikasi yang menerima mengerti dan memahami bahkan bisa memanipulasi data tersebut.

2.5.3 *Session Layer*

Session Layer mendefinisikan bagaimana memulai, mengontrol dan mengakhiri percakapan. *Layer 5* ini menjamin komunikasi antara *host*, yang berarti bahwa menetapkan cara untuk mengatur sesi antara aplikasi.

Di *Layer* ini kita temukan SQL, NFS, RPC. Biasanya sistem operasi yang bertanggung jawab untuk *Layer* yang satu ini.

2.5.4 *Transport Layer*

Transport Layer menjamin pengelolaan *circuit virtual* antara *host* yang mampu mengoreksi kesalahan. Ini berisikan serangkaian protokol dengan masalah-masalah transportasi antara *host*. Protokol-protokol ini dapat menyusun ulang aliran data paket jika terjadi kerusakan. *Layer 4* juga bertanggung jawab atas data yang masuk dari aliran yang berbeda untuk aplikasi yang berjalan pada *host* yang sama.

Di *Layer* ini kita menemukan TCP, UDP dan SPX. Fitur penting di *Layer* ini adalah kemampuan untuk mengoreksi kesalahan dan *Flow Control* dari *Router*. OSI *Layer 4* menyediakan layanan untuk *Layer 5*, yang berarti bahwa setelah data diterima dan di atur kembali sedemikian rupa kemudian diberikan ke *Layer* di atasnya untuk penanganan. *Layer 4* ini bertanggung jawab untuk membatasi kecepatan transmisi jaringan sehingga tidak terjadi *flood*. Ini disebut juga dengan *Flow Control*.

2.5.5 *Network Layer*

Layer 3 ini mendefinisikan pengiriman data dari ujung ke ujung (*EndToEnd*). Agar *compile* dapat diidentifikasi, *Layer 3* mendefinisikan alamat secara logis (Contoh IP). OSI *Layer 3* juga mendefinisikan bagaimana *routing* bekerja dan bagaimana *route* dipelajari oleh *router* untuk pengiriman paket-paket dan juga mendefinisikan fragmentasi paket, dimana hal ini merupakan

proses yang memecah paket ke unit yang lebih kecil agar dapat mengakomodasi media dengan ukuran yang lebih kecil (*Maximum Transmission Packets MTU*).

Pada umumnya di *Layer* ini kita menemukan IP dan IPX. Ketika kita berbicara tentang OSI *Layer* 3, kita harus berpikir tentang “*Routing*”. Sebagai contoh, *Layer* 3 adalah perangkat yang menjalankan protokol *routing* untuk lintasan

Router membuat keputusan *routing* berdasarkan tabel *routing* yang mereka miliki. Tabel *routing* itu sendiri merupakan kumpulan aturan yang mendefinisikan kemana data harus pergi dan alamat tertentu dalam sebuah jaringan.

2.5.6 Data Link

Layer 2 ini bertujuan untuk men-*transfer* data melalui media tertentu.

Contoh, IEEE 802.3 yang merupakan protokol untuk *ethernet*, di temukan di OSI *Layer* 2. *Hubs* dan *Switches* juga merupakan perangkat *Layer* 2 yang men-*transfer* paket-paket dari kabel tembaga. Pada *Layer* 2 ini kita akan menemukan protokol seperti ATM, *Frame Relay*, HDLC, PPP, FDDI.

Akan tetapi, yang perlu kita pahami di *Layer* ini adalah bahwa OSI *layer* 2 menentukan bagaimana paket yang di kirim ke link komunikasi. Ketika kita berbicara OSI *layer* 2, kita harus berpikir tentang “*Switching*”.

2.5.7 *Physical Layer*

Layer 1 berisi spesifikasi media fisik transmisi data yang digunakan protokol *link layer*. *Layer 1* adalah tentang konektor, pin, arus listrik, modulasi cahaya. Pada *Layer 1*, kita menemukan 802,3 *standart*, yang memiliki definisi tentang *pinout ethernet*, panjang kabel, tegangan. Lebih itu, kita menemukan spesifikasi pengkabelan *standar* untuk RJ45, RJ48, V.35, V.24. Ketika kita berbicara tentang lapisan 1, kita berpikir tentang “Kabel dan Konektor”

2.6 CobIT

Menurut ISACA (Information Systems Audit and Control Association)

CobIT (Control Objective for Information and Related Technology) adalah sebuah alat yang telah diterima secara internasional yang diorganisir menjadi sebuah kerangka kerja (framework) yang dapat digunakan para eksekutif untuk memastikan bahwa Teknologi Informasi yang mereka miliki membantu mereka dalam mencapai sasaran dan tujuannya. CobIT memastikan bahwa Teknologi Informasi bekerja secara efektif memungkinkan untuk meminimalkan risiko TI yang terkait dan memaksimalkan keuntungan dari investasi teknologi.

Menurut Sofana (2011), CobIT merupakan suatu cara untuk menerapkan *IT Governance*. CobIT berupa kerangka kerja yang harus digunakan oleh suatu organisasi bersamaan dengan sumber daya lainnya untuk membentuk suatu standar yang umum berupa panduan pada lingkungan yang lebih spesifik. Secara struktur, CobIT terdiri dari seperangkat *control objectives* untuk bidang teknologi infirmasi, dirancang untuk memungkinkan tahapan bagi audit.

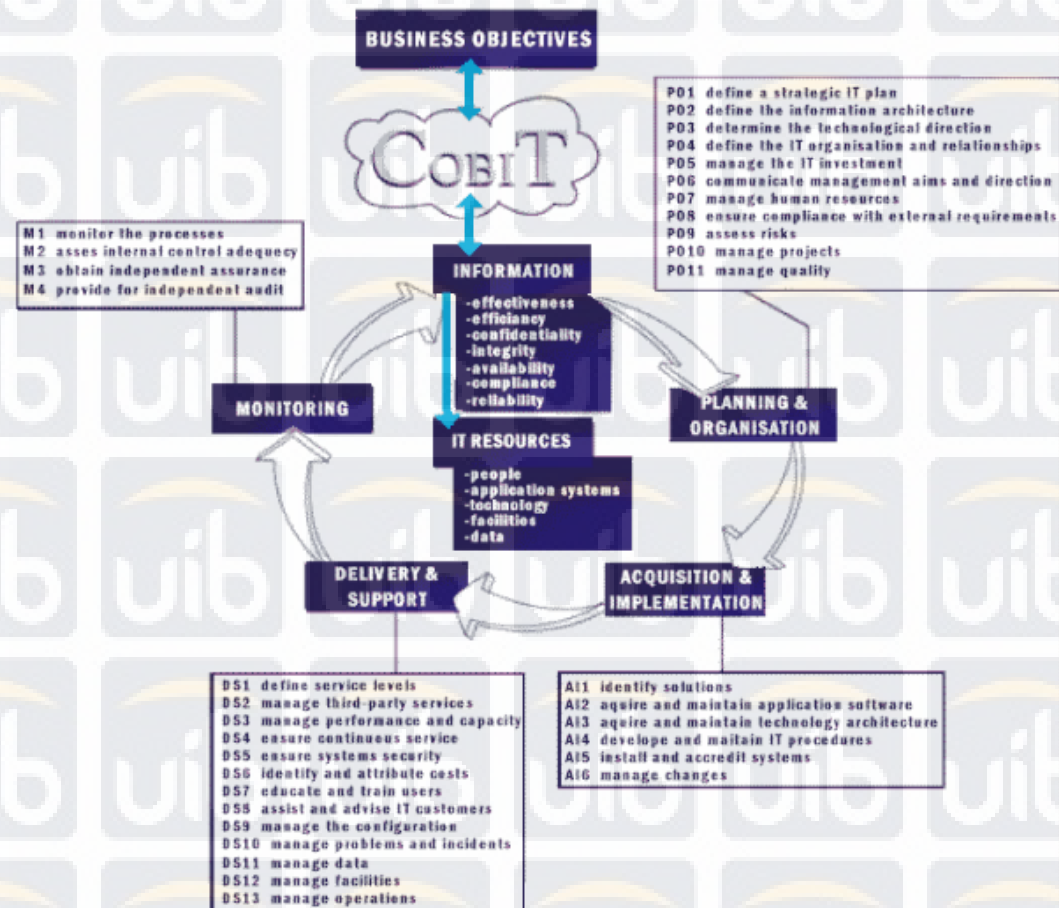
CobIT disusun oleh The IT Governance Institute (ITGI) dan Information System Audit and Control Foundation (ISACF) pada tahun 1992. Edisi pertama CobIT dipublikasikan pada tahun 1996, kemudian edisi kedua dari CobIT diterbitkan pada tahun 1998. Pada tahun 2000 dirilis cobIT 3.0, CobIT 4.0 pada tahun 2005 dan cobIT 4.1 pada tahun 2007. Kemudian terakhir CobIT 5.0 pada tahun 2012. CobIT merupakan kombinasi dari prinsip-prinsip yang telah ditanamkan dilengkapi dengan balance scorecard dan dapat digunakan sebagai acuan model (seperti COSO) dan disejajarkan dengan standar industri, seperti ITIL, CMM, BS779, ISO9000.

CobIT difokuskan pada apa yang diperlukan untuk mencapai pengelolaan dan pengendalian TI yang memadai, dan diposisikan pada tingkat tinggi. CobIT framework didasarkan pada prinsip untuk memberikan informasi yang dibutuhkan perusahaan untuk mencapai tujuannya, investasi yang diperlukan perusahaan, serta mengelola dan mengendalikan sumber daya IT menggunakan seperangkat proses yang terstruktur untuk meberikan layanan informasi yang dibutuhkan perusahaan.

CobIT berguna bagi Auditor untuk mendukung atau memperkuat opini yang dihasilkan dan memberikan saran kepada manajemen atas pengendalian internal yang ada. Bagi Manajemen untuk membantu mereka menyeimbangkan antara resiko dan investasi pengendalian dalam sebuah lingkungan TI yang sering tidak dapat diprediksi. Sedangkan bagi user, CobIT berguna untuk memperoleh keyakinan atas kehandalan sistem aplikasi yang digunakan.

2.6.1 CobIT Framework

Secara keseluruhan, hubungan antara *Business Objective*, *IT Governance*, *Information*, *IT Resource*, dengan 4 domain dan 34 *high level control objectives*.



Gambar 2.2 CobIT Framework

2.6.1.1 Kriteria Informasi CobIT

Menurut CobIT, untuk memenuhi tujuan bisnis perusahaan informasi harus sesuai dengan kriteria pengendalian tertentu yang disebut sebagai kriteria informasi CobIT, yaitu :

1. Effectiveness (Efektifitas)

Informasi yang diperoleh harus relevan dan berkaitan dengan proses bisnis, disampaikan tepat waktu, tepat, konsisten, dan dapat dipercaya.

2. Efficiency (Efisiensi)

Penyediaan informasi melalui penggunaan sumber daya (yang paling produktif dan ekonomis) yang optimal.

3. Confidentiality (Kerahasiaan)

Berkaitan dengan proteksi pada informasi penting dari pengungkapan yang tidak sah atau pihak-pihak yang tidak memiliki otorisasi.

4. Integrity (Integritas)

Berkaitan dengan keakuratan dan kelengkapan informasi serta validitas yang sesuai dengan nilai-nilai bisnis dan ekspektasi.

5. Availability (Ketersediaan)

Fokus terhadap ketersediaan informasi ketika diperlukan dalam proses bisnis, baik sekarang maupun di masa yang akan datang. Ini juga terkait dengan pengamanan sumber daya yang diperlukan dan terkait.

6. Compliance (Kepatuhan)

Pemenuhan informasi yang sesuai dengan ketentuan hukum, peraturan dan rencana perjanjian/kontrak untuk proses bisnis.

7. Reliability (Handal)

Pemberian informasi yang tepat bagi manajemen untuk mengoperasikan perusahaan dan pemenuhan kewajiban mereka untuk membuat laporan keuangan dan tanggung jawab kepada pemerintah.

2.6.1.2 Elemen *IT Resource*

Elemen-elemen sumber daya TI merupakan hal yang sangat penting dalam pencapaian tujuan bisnis, karena itu dibutuhkan dukungan sumber daya informasi yang memadai. Fokus terhadap pengelolaan sumber daya teknologi informasi dalam cobIT 4.1 diantaranya :

a. *Application* (Aplikasi)

Merupakan sistem otomatis yang digunakan dan prosedur manual mengenai proses informasi.

b. *Information* (Informasi)

Merupakan data, dalam segala bentuk yang melalui tahap input, processed dan output dihasilkan oleh sistem informasi dalam berbagai bentuk yang nantinya akan digunakan oleh perusahaan.

c. *Infrastructure* (Infrastruktur)

Merupakan dan fasilitas (*hardware, operating systems, database management system, networking, multimedia* dan lingkungan pendukung lainnya) yang dapat memproses aplikasi.

d. *People* (Manusia)

Personil yang dibutuhkan untuk perencanaan, mengorganisasikan, memperoleh mengimplementasikan, menyampaikan, mendukung, mengawasi dan mengevaluasi sistem layanan informasi.

2.6.1.3 Komponen *Control Objectives*

Framework CobIT disusun dengan karakteristik yang berfokus pada bisnis (*business-focused*), berorientasi pada proses (*processoriented*), berbasis pada pengendalian (*controls-based*) dan terarah kepada pengukuran (*measurement-driven*). CobIT framework 4.1 terdiri dari 34 high level control objectives dan kemudian mengelompokkan proses tersebut menjadi 4 domain, keempat domain tersebut adalah: *Planning and Organization* (10 proses), *Acquisition and Implementation* (7 proses), *Delivery and Support* (13 proses), dan *Monitoring and Evaluation* (4 proses), yang mencakup:

1. Plan and Organise (Perencanaan dan Organisasi)

Mencakup strategi, taktik dan identifikasi kontribusi terbaik TI demi pencapaian tujuan perusahaan. Domain ini meliputi pertanyaan-pertanyaan sebagai berikut :

- a) Apakah proses TI dan strategi bisnis telah sesuai?
- b) Apakah perusahaan mencapai penggunaan yang optimum dengan sumber dayanya?
- c) Apakah setiap karyawan di perusahaan memahami tujuan TI?
- d) Apakah resiko TI dipahami dan dikelola?
- e) Apakah kualitas sistem TI sesuai dengan kebutuhan bisnis?

2. Acquire and Implement (Pengadaan dan Implementasi)

Untuk merealisasikan strategi TI, perlu dilakukan pengidentifikasian, pengembangan dan perolehan solusi TI, sesuai dengan yang akan diimplementasikan dan diintegrasikan ke dalam proses bisnis. Domain ini meliputi pertanyaan-pertanyaan sebagai berikut :

- a) Apakah proyek baru kemungkinan akan memberikan solusi yang dibutuhkan?
- b) Apakah proyek baru kemungkinan akan dikirim tepat waktu sesuai dengan anggaran?
- c) Apakah sistem baru dapat bekerja dengan baik ketika diimplementasikan?
- d) Apakah perubahan dilakukan tanpa mengganggu operasi bisnis yang sedang berjalan?

3. Deliver and Support (Pengiriman Layanan dan Dukungan)

Domain ini berfokus terhadap penyampaian jasa yang sesungguhnya diperlukan, termasuk penyediaan layanan, manajemen keamanan dan kontinuitasnya, jasa dukungan kepada user dan manajemen data dan fasilitas operasi. Domain ini meliputi pertanyaan-pertanyaan sebagai berikut :

- a) Apakah jasa TI yang disampaikan sejalan dengan prioritas bisnis?
- b) Apakah biaya TI teroptimisasi?
- c) Apakah sistem TI sistem bekerja secara produktif dan aman?
- d) Apakah terdapat kontrol demi kerahasiaan, integritas dan ketersediaan yang baik terhadap keamanan informasi?

4. Monitor and Evaluate (Pengawasan dan Evaluasi)

Berkenaan dengan manajemen kinerja, pemantauan internal control, kepatuhan terhadap regulasi dan pelaksanaan tata kelola. Domain ini meliputi pertanyaan-pertanyaan sebagai berikut:

- a) Apakah kinerja TI diukur untuk mendeteksi permasalahan sebelum terlambat?
- b) Apakah pihak manajemen memastikan bahwa internal control efektif dan efisien?
- c) Dapatkah kinerja TI dihubungkan dengan tujuan perusahaan?
- d) Apakah terdapat kontrol demi kerahasiaan, integritas dan ketersediaan yang baik terhadap keamanan informasi?

2.6.2 Manfaat Penerapan CobIT

Menurut The IT Governance Institute (ITGI), manfaat dari penerapan CobIT sebagai kerangka tata kelola TI meliputi:

- 1 Penggunaan bahasa yang umum bagi para eksekutif, manajemen dan profesional TI.
- 2 Pemahaman yang lebih baik tentang bagaimana bisnis dan TI dapat bekerja sama untuk keberhasilan pengiriman inisiatif TI.
- 3 Peningkatan efisiensi dan optimalisasi biaya.
- 4 Mengurangi risiko operasional.
- 5 Pengembangan kebijakan yang jelas.
- 6 Audit yang lebih efisien dan sukses.
- 7 Kepemilikan dan tanggung jawab yang jelas, berdasarkan proses orientasi.

2.6.3 Maturity Model

Menurut ISACA maturity model merupakan alat bantu yang dapat digunakan untuk memetakan status maturity proses (dalam skala 0-5), diantaranya:

1. Skala 0 – Not Existence
Perusahaan tidak menyadari pentingnya membuat perencanaan strategis di bidang teknologi informasi. Dalam skala ini penting untuk dilakukan evaluasi pengendalian dan dijadikan sebagai temuan yang penting.

2. Skala 1 – Initial

Perusahaan telah menyadari akan pentingnya pembuatan perencanaan strategis di bidang teknologi informasi. Namun, tidak ada proses yang distandarisasi; perencanaan, perancangan dan manajemen masih belum teroganisir dengan baik. Dalam skala ini keperluan untuk dijadikan temuan, karena tingkat kemungkinan terjadinya resiko tidak sebesar skala 0.

3. Skala 2 – Repeatable

Perusahaan telah menetapkan prosedur untuk dipatuhi oleh karyawan, namun belum dikomunikasikan dan belum adanya pemberian latihan formal kepada setiap karyawan mengenai prosedur dan tanggung jawab diberikan sepenuhnya kepada individu sehingga pemberian kepercayaan sepenuhnya kemungkinan dapat terjadi penyalahgunaan.

4. Skala 3 – Defined

Proses telah didokumentasikan dan telah dikomunikasikan, serta dilaksanakan berdasarkan metode pengembangan sistem komputerisasi yang baik, namun belum ada proses evaluasi terhadap sistem tersebut, sehingga masih ada kemungkinan terjadinya penyimpangan.

5. Skala 4 – Managed

Proses komputerisasi telah dapat dimonitor dan dievaluasi dengan baik, manajemen proyek pengembangan sistem komputerisasi sudah dijalankan dengan lebih teroganisir.

6. Skala 5 – Optimised

Best Practices (pedoman terbaik) telah diikuti dan diotomatisasi pada sistem berdasarkan proses yang terencana, terorganisir dan menggunakan metodologi yang tepat.