



**IKI-83408T : Proteksi dan Teknik Keamanan Sistem Informasi**

**Suplemen Bahan Ajar IKI-83408T**  
**Domain: Security Architecture & Models**  
**Kelompok 128M**

**Oleh :**

1. Ririn Ikana Desanti (7204000608)
2. M. Feriza Yoga I.A. (720400050Y)
3. Arif Dermawan Isnandar (7204000214)

**MAGISTER TEKNOLOGI INFORMASI**  
**PROGRAM PASCASARJANA**  
**UNIVERSITAS INDONESIA**  
**2005**

## DAFTAR ISI

DAFTAR ISI .....	1
DAFTAR GAMBAR .....	3
DAFTAR TABEL.....	4
BAB I PENGANTAR ARSITEKTUR DAN MODEL KEAMANAN.....	5
1. Arsitektur Keamanan .....	5
2. Arsitektur Komputer .....	5
2.1 Memory .....	5
2.2 Daur Eksekusi Instruksi .....	7
2.3 Struktur <i>Input/Output</i> (Masukan/Keluaran).....	9
3. Perangkat Lunak.....	10
4. Open System.....	12
5. Closed System.....	13
6. Mekanisme Proteksi .....	13
6.1 Rings .....	14
6.2 Security Modes .....	14
BAB II MODEL KEAMANAN INFORMASI.....	16
1. Access Control Models .....	16
1.1 The Access Matrix .....	16
1.2 Take-Grant Model.....	18
1.3 Bell-LaPadula Model.....	19
2. Integrity Models .....	23
2.1 The Biba Integrity Model.....	23
2.2 The Clark-Wilson Integrity Model.....	24
3. Information Flow Models.....	24
3.1 Non-Interference Model .....	25
3.2 Composition Theories.....	25
BAB III PENJAMINAN .....	27
1. Kriteria Evaluasi.....	27
2. Sertifikasi dan Akrediatasi .....	28
3. DITSCAP dan NIACAP .....	28
3.1 DITSCAP .....	28
3.2 NIACAP .....	29
3.3 Systems Security Engineering - Capability Maturity Model (SSE-CMM)	29
BAB IV IMPLEMENTASI CONTOH KASUS PADA UKM.....	33
1. Latar Belakang.....	33
2. Struktur Organisasi Cyber Campus .....	34
3. Aplikasi yang digunakan .....	35

4.	Sistem Kontrol Akses.....	35
5.	Contoh SOP: .....	45
	BIBLIOGRAPHY.....	54

## DAFTAR GAMBAR

Gambar 1.1 Memori Hirarki Sebuah Komputer.....	6
Gambar 1.2 A Typical Machine Cycle .....	8
Gambar 1.3 Instruction Pipelining.....	8
Gambar 1.4 Proses Very-Long Instruction Word (VLIW) .....	9
Gambar 1.5 Proteksi Ring .....	14
Gambar 2.1. Model Take-Grant [RON05: 304] .....	19
Gambar 2.2. Perpindahan Posisi Dibatasi Oleh Fungsi F Dan Input X. [RON05:305].....	20
Gambar 2.3. Biba Model Axioms [RON05: 306].....	22
Gambar 2.4 Model Alir Informasi [RON05: 309].....	25
Gambar 4.1 Struktur Organisasi Cyber Campus .....	34

## DAFTAR TABEL

Tabel 2.1 Contoh Matriks Akses .....	16
Tabel 4.1 Daftar Nama dan Jabatan.....	35
Tabel 4.2 Tabel <i>Access Control Matrix Model</i> Aplikasi Aset Logical.....	37
Tabel 4.3 Tabel Access Control Matrix Model aset fisik peralatan TI.....	38

# BAB I

## PENGANTAR ARSITEKTUR DAN MODEL KEAMANAN

Tujuan dari domain ini adalah untuk mempelajari konsep, prinsip dan standar untuk merancang dan mengimplementasikan aplikasi, sistem operasi dan sistem yang aman. Penerapan *security architecture* dan model yang baik akan sangat membantu keamanan sistem perusahaan secara keseluruhan.

### 1. Arsitektur Keamanan

Arsitektur keamanan menggabungkan kombinasi antara kebijakan-kebijakan, teknologi, *practices*, dan adanya kesadaran perusahaan akan pentingnya mengamankan data, transaksi, dan komponen infrastruktur. Bagi sebagian besar perusahaan, arsitektur keamanan harus memberikan sebuah *framework* yang mampu mengintegrasikan produk dan peralatan yang tersedia untuk bisa memenuhi kebutuhan perusahaan dan mengantisipasi perkembangan bisnis yang terjadi.

Di dalam bagian arsitektur keamanan ini, ada beberapa point yang akan dibahas yaitu:

1. Arsitektur Komputer
2. Open System
3. Closed System
4. Mekanisme Proteksi

### 2. Arsitektur Komputer

Pada intinya arsitektur komputer ini merupakan ilmu dalam memilih dan menghubungkan antar komponen-komponen *hardware* untuk menciptakan sebuah komputer yang bisa memenuhi kebutuhan fungsional dan *performance*, dan juga perkiraan biaya. Jadi ilmu ini bukan sekedar bagaimana menggunakan komputer untuk merancang suatu bangunan. Untuk lebih memahami hal tersebut maka harus lebih dulu memahami komponen-komponen tersebut.

#### 2.1 Memory

*Memory* memiliki beberapa tipe sebagai berikut:

##### 1. **Random Access Memory (RAM)**

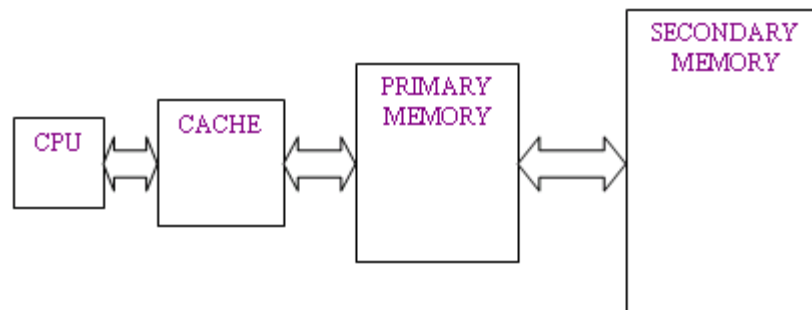
Memori yang dapat langsung dialamatkan dan data yang disimpan didalam memori ini dapat diubah. RAM bersifat *volatile* (sementara) sehingga jika tidak ada lagi *power* pada sistem maka datanya akan hilang.

##### 2. **Cache Memory**

RAM yang relatif lebih sedikit namun sangat berkecepatan tinggi. Memori ini memegang data dan instruksi dari memori primari yang memiliki probabilitas akses yang tinggi selama proses eksekusi program.

3. **RDRAM Memory (Rambus RDRAM)**  
Memori ini menggunakan teknologi RSL (*Rambus Signaling Level*) dan menyediakan sistem berkapasitas 16MB sampai 2GB pada kecepatan lebih dari 1066MHz.
4. **Programmable Logic Device (PLD)**  
Sebuah sirkuit terintegrasi dengan koneksi atau jembatan *internal logic* yang dapat diubah melalui proses pemrograman. Contohnya yaitu *Read Only Memory (ROM)*, *Programmable Array Logic (PAL)*, *Complex Programmable Logic Device (CPLD)*, dan *Field Programmable Gate Array (FPGA)*.
5. **Read Only Memory (ROM)**  
Tempat penyimpanan yang bersifat *non-volatile* dan lokasinya dapat langsung dialamatkan. *Non-volatile* ini akan tetap menyimpan informasi atau data walaupun sistem dalam keadaan mati. Ada beberapa tipe dari ROM yaitu EPROMs (*Erasable, Programmable Read Only Memories*), EAROMs (*Electrically Alterable Read Only Memories*), EEPROMs (*Electrically Erasable Programmable Read Only Memories*), memori *flash*.
6. **Real or Primary Memory**  
Memori yang langsung dialamatkan oleh CPU dan digunakan untuk penyimpanan instruksi dan data yang berhubungan dengan program yang sedang dieksekusi.
7. **Secondary Memory**  
Tipe memori yang lebih lambat yang menyediakan penyimpanan *non-volatile*. Contohnya adalah *magnetic disk*.
8. **Sequential Memory**  
Memori yang berisi informasi yang bisa dibaca secara sekuensial dimulai dari awal. Contohnya adalah membaca informasi dari *magnetic tape*.
9. **Virtual Memory**  
Tipe ini menggunakan memori *secondary* untuk memberikan ruang alamat yang lebih besar dan jelas bagi CPU.

Gambar 1 dibawah ini adalah gambar dari memori hirarki:



**Gambar 1.1 Memori Hirarki Sebuah Komputer**

Ada beberapa cara bagaimana CPU mengalamatkan memori. Dibawah ini beberapa model yang sering digunakan:

1. **Register addressing:**
2. **Direct addressing**
3. **Absolute addressing**
4. **Indexed addressing**
5. **Implied addressing**
6. **Indirect addressing**

Pengamanan memori dimaksudkan untuk mencegah sebuah program mengakses dan mengubah isi *memory space* milik program lain. Pengamanan memori ini dijalankan oleh sistem operasi atau oleh mekanisme *hardware*.

## 2.2 Daur Eksekusi Instruksi

Daur dari sebuah mesin terdiri dari dua tahap yaitu mengambil (*fetch*) dan menjalankan (*execute*). Pada tahap *fetch*, CPU akan memberikan alamat dari instruksi kepada memori, dan mengambil instruksi yang ada pada alamat tersebut. Lalu pada tahap *execute*, instruksi diartikan kemudian dieksekusi.

Sebuah mesin atau komputer dapat berada pada beberapa *state*. Saat komputer mengeksekusi instruksi, situasi ini disebut *operation state*. Lalu pada saat program aplikasi dijalankan, mesin berada pada *problem state*. Pada saat komputer menjalankan instruksi khusus (*privilege*), maka komputer berada pada *supervisory state*. Dan komputer bisa berada pada kondisi *wait state* jika sedang mengakses memori yang lambat, jadi ada jeda waktu menunggu. Untuk meningkatkan kecepatan dari mengambil dan mengeksekusi instruksi, ada beberapa pendekatan yang bisa dilakukan yaitu:

**Pipelining:** meningkatkan kinerja komputer dengan cara saling *overlap* tahapan dari instruksi yang berbeda.

**Complex Instruction Set Computer (CISC):** menggunakan instruksi yang menyajikan banyak operasi pada tiap instruksi yang ada.

**Reduced Instruction Set Computer (RISC):** menggunakan instruksi yang lebih mudah dan meminta *clock cycle* yang lebih sedikit untuk dijalankan. Pendekatan ini menyebabkan peningkatan kecepatan memori dan komponen prosesor lainnya.

**Scalar Processor:** prosesor yang menjalankan satu instruksi pada satu waktu tertentu.

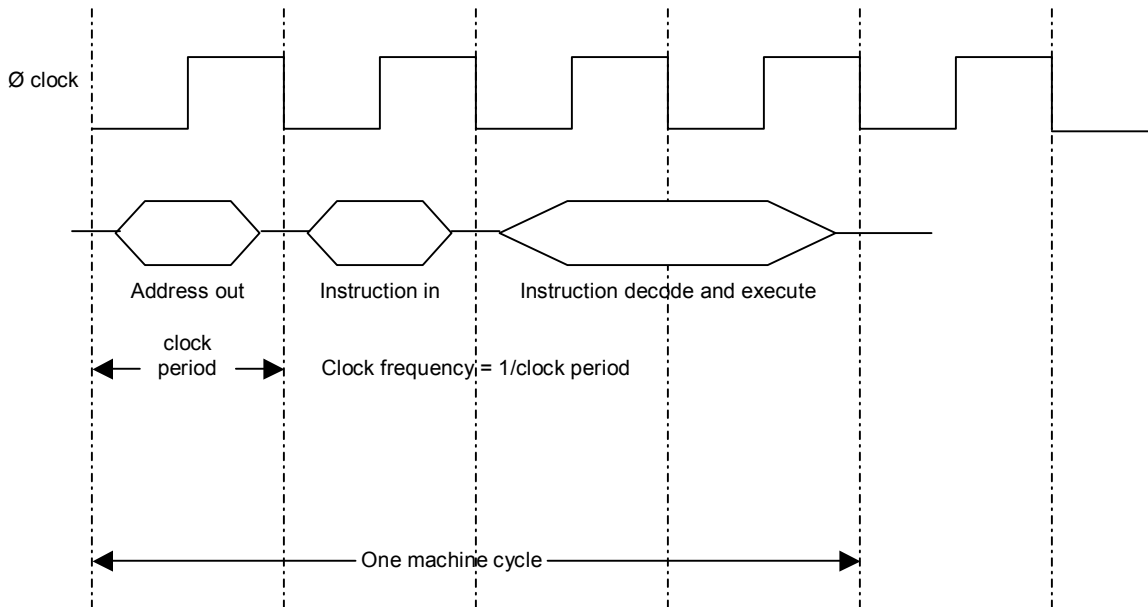
**Superscalar Processor:** prosesor yang memungkinkan jalannya beberapa instruksi sekaligus dalam tahap *pipeline* yang sama atau juga berbeda.

**Very-Long Instruction Word (VLIW) Processor:** prosesor dimana sebuah instruksi menentukan lebih dari satu operasi yang terjadi bersamaan.

**Multi-programming:** mengeksekusi dua atau lebih program secara bersama pada sebuah CPU dengan cara saling bertukar antar program.

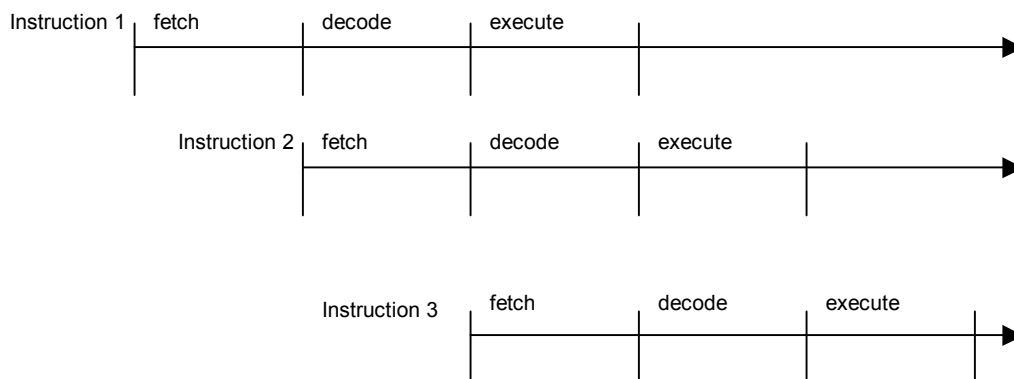
**Multi-tasking:** mengeksekusi dua atau lebih sub program atau tugas pada waktu yang sama pada sebuah CPU dengan cara saling bertukar antar tugas.

**Multi-processing:** mengeksekusi dua atau lebih programs pada saat yang sama pada prosesor yang berbeda-beda.

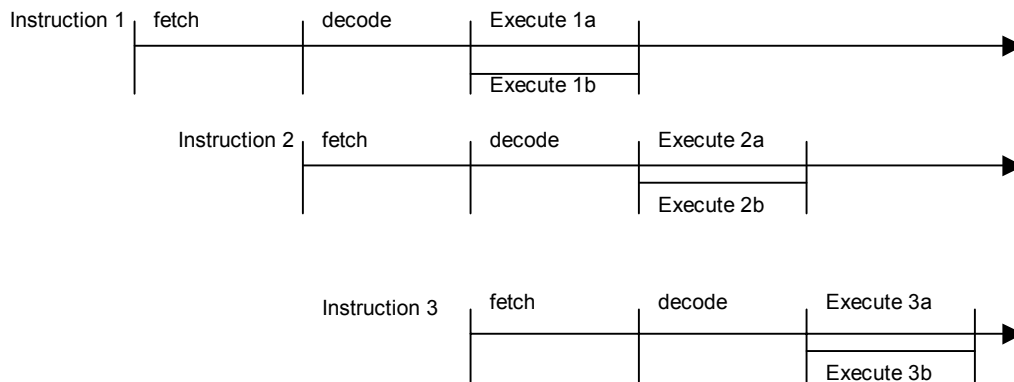


**Gambar 1.2 A Typical Machine Cycle**

Setelah memeriksa siklus mesin dasar, hal ini sangat nyata bahwa ada peluang untuk menambah kecepatan mendapatkan kembali dan mengeksekusi instruksi. Beberapa metode ini mencakup meng-overlap fetch dan mengeksekusi siklus, mengeksplorasi peluang untuk parallelism., mengantisipasi instruksi yang akan dieksekusi kemudian, fetching dan decoding instruksi lebih jauh, dan lain-lain.



**Gambar 1.3 Instruction Pipelining**



**Gambar 1.4** Proses Very-Long Instruction Word (VLIW)

### 2.3 Struktur *Input/Output* (Masukan/Keluaran)

Sebuah prosesor akan berkomunikasi dengan peralatan lain melalui alat *interface* yang disebut adapter *interface input/output* (I/O). Ada sebuah rancangan yang disebut *memory-mapped I/O*, dimana sebuah adapter diberikan alamat dalam memori sehingga akan mengambil alamat memori yang lebih khusus. Kelebihan dari pendekatan ini adalah bahwa CPU melihat tidak ada perbedaan pada setiap instruksi yang ada untuk adapter I/O dan lokasi memori yang lainnya. Oleh karena itu, semua instruksi komputer yang berhubungan dengan memori akan dapat digunakan oleh alat I/O.

Sedangkan pada I/O yang tersembunyi (*isolated I/O*), sinyal khusus pada bus mengindikasikan bahwa sebuah operasi I/O sedang dijalankan. Kelebihan dari I/O yang tersembunyi ini adalah bahwa alamat ini tidak akan membuang-buang alamat yang bisa digunakan untuk memori. Sedangkan kekurangannya adalah pengaksesan dan manipulasi data I/O terbatas pada sejumlah kecil instruksi I/O tertentu di dalam sekumpulan instruksi untuk prosesor. Keduanya, *memory-mapped I/O* dan *isolated I/O* dikenal juga sebagai *programmed I/O*.

*Direct Memory Access* (DMA) merupakan salah satu pilihan untuk mempercepat proses prosesor. Dengan DMA, data akan ditransfer secara langsung ke dan dari memori tanpa harus melalui CPU. Transfer data dengan DMA sangat terbatas oleh waktu daur memori. Jalur transfer data antara memori dan peralatan *peripheral* disebut dengan *channel*.

*Interrupt* dapat digunakan sebagai alternatif lain untuk perpindahan data. Pada proses *interrupt*, sinyal dari luar akan menginterupsi alur program dan meminta *service*. Saat CPU menerima permintaan interupsi, CPU akan menyimpan kondisi yang sedang berjalan dari sebuah program lalu akan beralih ke program lain yang menyediakan interupsi. Jika layanan interupsi telah selesai, CPU akan menyimpan kembali kondisi terakhir dari program yang awal dan akan berlanjut memproses.

### 3. Perangkat Lunak

CPU sebuah komputer didesain untuk mendukung eksekusi sebuah set instruksi yang berasosiasi dengan komputer tersebut. Set ini terdiri dari berbagai macam instruksi seperti ADD WITH CARRY, ROTATE BITS LEFT, MOVE DATA, dan JUMP TO LOCATION X. Setiap instruksi direpresentasikan sebagai kode biner dimana decoder instruksi dari CPU didesain untuk mengenali dan mengeksekusinya. Instruksi ini didefinisikan sebagai instruksi bahasa mesin. Kode setiap instruksi bahasa mesin berasosiasi dengan sebuah bahasa Inggris yang mudah diingat untuk memudahkan orang-orang bekerja dengan kode-kode tersebut. Set instruksi dasar komputer yang mudah diingat ini disebut sebagai bahasa perakitan (assembly language) dimana bahasa ini spesifik terhadap komputer-komputer tertentu. Jadi, ada sebuah korespondensi satu-satu untuk setiap instruksi bahasa perakitan pada setiap instruksi bahasa mesin. Sebagai contoh, pada sebuah kata instruksi 8 bit yang sederhana komputer, kode biner untuk instruksi bahasa mesin ADD WITH CARRY akan menjadi 10011101, dan korespondensi yang mudah diingat adalah ADC. Seorang programmer yang menulis kode ini pada level bahasa mesin akan menulis kodenya menggunakan kata yang mudah diingat untuk setiap instruksinya. Lalu kode tersebut akan melewati program lain yang disebut assembler yang akan menjalankan transaksi satu ke satu kode bahasa perakitan ke kode bahasa mesin. Kode yang dihasilkan oleh assembler yang berjalan pada komputer disebut source code. Perangkat lunak assembler bisa berada pada komputer yang sedang diprogram dan ini disebut resident assembler. Jika assembler sedang berjalan pada komputer lain, assembler ini disebut cross assembler. Cross assembler bisa berjalan pada berbagai tipe dan model komputer. Sebuah disassembler berkebalikan fungsi dengan sebuah assembler dengan menterjemahkan bahasa mesin menjadi bahasa perakitan.

Jika sebuah kelompok statemen-statemen bahasa rakitan digunakan untuk melaksanakan satu fungsi spesifik, mereka dapat didefinisikan dengan assembler dengan sebuah nama yang disebut MAKRO. Kemudian, sebagai ganti menulis daftar statemen-statemen, MAKRO dapat dipanggil, menyebabkan assembler menyisipkan statemen-statemen yang sesuai.

Oleh karena keinginan untuk menulis perangkat lunak pada level yang lebih tinggi, statemen English-like, bahasa level tinggi digunakan. Pada bahasa ini, satu statemen biasanya memerlukan sejumlah instruksi bahasa mesin untuk implementasinya. Oleh karena itu, tidak seperti bahasa rakitan, ada hubungan satu ke banyak dari instruksi bahasa level tinggi ke instruksi bahasa mesin. Pascal, FORTRAN, BASIC, dan Java adalah contoh bahasa level tinggi. Bahasa level tinggi diterjemahkan ke instruksi bahasa mesin yang bersesuaian melalui baik sebuah program interpreter atau compiler. Sebuah interpreter beroperasi pada setiap statemen sumber bahasa level tinggi secara tersendiri dan menjalankan operasi yang sudah diindikasikan dengan cara mengeksekusi urutan instruksi bahasa mesin yang telah ditentukan. Oleh karena itu, instruksi-instruksi ini dieksekusi sesegera mungkin. Java dan BASIC adalah contoh dari

bahasa interpreter. Secara kontras, sebuah compiler menterjemahkan seluruh program program perangkat lunak ke dalam perintah bahasa mesin yang bersesuaian. Instruksi ini lalu di muat kedalam memori komputer dan lalu dieksekusi sebagai sebuah paket program. FORTRAN adalah sebuah contoh dari sebuah bahasa compiler. Dari sudut pandang keamanan, sebuah program compiler tidak terlalu diinginkan dibandingkan dengan sebuah interpreter karena kode yang membahayakan bisa menempati suatu tempat pada kode compiler, dan ini susah untuk dideteksi dalam program yang sangat besar.

Bahasa level tinggi dikelompokkan dalam 4 kelompok generasi, dan mereka di beri nama sebagai Generation Language (GL). Berikut adalah daftar bahasa-bahasanya:

- 1 GL. Sebuah bahasa mesin komputer
- 2 GL. Sebuah bahasa perakitan
- 3 GL. FORTRAN, BASIC, PL/1, dan Bahasa C
- 4 GL. NATURAK, FOCUS, dan bahasa query database.
- 5 GL. Prolog, LISP, dan bahasa kecerdasan buatan lainnya yang memproses simbol atau menerapkan logika predikat.

Program (atau sekumpulan program) yang mengontrol sumber daya dan operasi komputer disebut sebagai Sistem Operasi (OS). Sistem operasi menjalankan manajemen proses, manajemen memori, manajemen file sistem, dan manajemen I/O. Windows XP, Windows 2000, Linux dan Unix adalah beberapa contoh sistem operasi.

Sistem operasi berkomunikasi dengan sistem I/O melalui sebuah controller. Controller adalah sebuah perangkat yang melayani sebagai interface kepada periferal dan menjalankan perangkat lunak tertentu untuk mengelola pertukaran informasi dan operasi dari sebuah disk drive.

Pada penerapannya di usaha kecil dan menengah, pemilihan sistem komputer dan sistem operasi mejadi isu yang ramai diperdebatkan. Dari sekian banyak perdebatan sistem operasi yang ada, Linux menjadi salah satu pilihan usaha kecil dan menengah.

Jika kita sudah menetapkan diri untuk menggunakan sistem komputer dalam membantu bisnis, maka langkah pertamanya adalah menentukan jenis komputer yang akan dipakai. Pemilihan komputer sebetulnya tidak terlalu sulit, karena dengan anggaran sekitar empat juta rupiah, kita sudah bisa mendapatkan server yang cukup tangguh, mampu menjalankan sistem tersebut dengan baik.

Intel Pentium 4 kecepatan 2,4 GHz, memori 256MB, hard disk 40GB sudah merupakan perangkat yang ideal yang bisa dipakai sebagai server. Kalau memang anggarannya terbatas, pilihan lainnya bisa menggunakan prosessor AMD atau Transmeta yang semakin lama semakin populer.

Berikutnya, kita harus menentukan sistem yang akan dipakai, apakah cukup menggunakan satu komputer, beberapa komputer sebagai sistem jaringan komputer,

dikenal dengan nama Local Area Network (LAN), atau bahkan harus menerapkan Wide Area Network (WAN) jika letak gedungnya berjauhan satu sama lain.

Komputer yang kita beli tidak akan jalan sendiri tanpa sistem operasi, dan seperti kita ketahui, sistem operasi komputer yang paling banyak dipakai saat ini terdiri dari dua jenis, yaitu Microsoft Windows 2000 Server atau Linux. Kalau usaha kita dapat menyisihkan anggaran yang cukup, maka kita bisa membeli lisensi Microsoft Windows yang harganya bisa sampai ribuan dolar Amerika, sementara jika kita menggunakan Linux, kita tidak perlu membeli lisensi sistem operasinya, karena Linux merupakan sistem operasi yang bisa didapatkan dengan cuma-cuma.

Perdebatan dari kedua sistem ini tidak habis-habisnya, tetapi satu kenyataan bahwa pada akhirnya keduanya akan menuju ke satu titik, yaitu kepuasan pelanggan, dalam hal kemudahan dan kemampuan yang tinggi akan segala fungsinya.

Setelah semua infrastruktur kita sediakan, langkah berikutnya adalah menentukan pemakaian program aplikasi yang diinginkan. Pada saat ini, sudah lebih dari seratus produk program bisnis yang tersedia di pasaran dari yang nyaris diberikan cuma-cuma, sampai yang harga yang mencapai puluhan juta, semuanya tergantung pada kebutuhan kita.

Mahal-murahnya program yang akan dibeli tergantung dari fasilitas yang disediakan oleh pembuat programnya. Misalnya, ada program yang hanya bisa jalan di satu komputer, atau programnya bisa dihubungkan ke sistem bank, sehingga pemeriksaan buku bank menjadi lebih mudah

Ada pula sistem yang dibuat dalam standar internet, sehingga komputer kita bisa berhubungan dengan komputer lain yang berada di benua berbeda.

Dengan adanya jaringan internet, maka kebutuhan server untuk pelaku bisnis skala menengah ke bawah ini juga makin bertambah, yaitu dengan penambahan fungsi e-mail yang merupakan sarana terpenting dalam berkomunikasi dengan berbagai pihak, sudah tentu dengan tambahan fungsi; cepat dan murah.

#### **4. Open System**

*Open system* adalah sistem yang bersifat *vendor-independent* yang telah mengeluarkan spesifikasi dan interface dengan tujuan memperbolehkan operasi dengan produk dari vendor lain. *Open system* dibuat dengan peralatan dari beberapa manufaktur yang telah disesuaikan dengan standar industri.

Salah satu manfaat dari *open system* adalah bahwa itu akan direview dan dievaluasi oleh pihak yang independen. Jika pada lingkungan bisnis, dengan menggunakan *open system* maka yang akan didapat adalah:

1. **Manufaktur** dapat memperluas bisnis mereka dan meningkatkan keuntungan perusahaan dengan berkompetisi di dalam pasar terbuka yang mengadopsi dan menghargai kualitas dan inovasi.
2. **Integrator** dapat menawarkan pelanggan lebih banyak pilihan dengan menetapkan sistem *best-of-breed* dibandingkan dengan sistem vendor tunggal. Mereka juga bisa merancang dan mempersiapkan sistem dengan lebih mudah karena hanya sedikit komponen yang harus diintegrasikan.
3. **End user** dapat lebih berhemat: mereka bisa mengurangi biaya sistem, karena pasar terbuka telah mengadopsi persaingan harga yang lebih besar; mereka bisa mengurangi biaya produksi dengan membuat standarisasi terhadap spesifikasinya; dan juga mereka bisa mengurangi biaya daur hidup sistem, mulai dari instalasi sampai pada pengembangan lebih luas.

## 5. Closed System

*Closed system* menggunakan perangkat keras dan atau perangkat lunak yang bersifat *vendor-dependent*, yang biasanya tidak kompatibel dengan sistem atau komponen lain. *Closed system* tidak bersifat independen dalam pengujian dan mungkin memiliki kelemahan (*vulnerability*) yang tidak diketahui atau tidak dikenal.

## 6. Mekanisme Proteksi

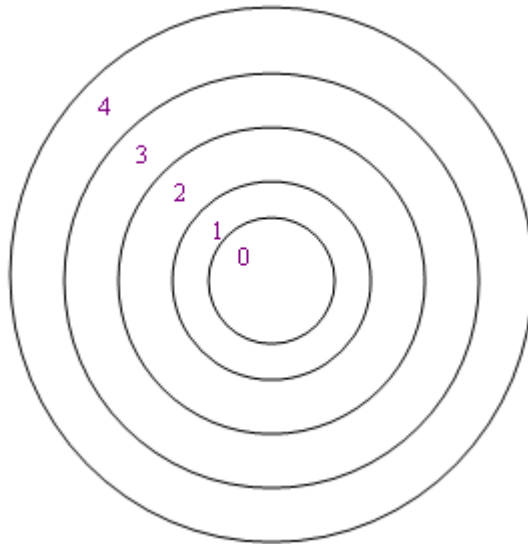
Proteksi domain mengacu kepada eksekusi dan pengalokasian memori terhadap setiap proses, dimana domain ini dapat diperluas ke virtual memory yang meningkatkan ukuran nyata dari memori menggunakan media penyimpanan berupa disk. Tujuan dari membangun proteksi domain ini adalah untuk mengamankan program dari modifikasi yang tidak berhak dan dari intervensi pihak luar.

*Trusted Computing Base (TCB)* adalah kombinasi dari mekanisme proteksi di dalam sistem komputer yang terdiri dari hardware, software, dan firmware yang dipercaya untuk menjalankan kebijakan keamanan. Ukuran dari suatu keamanan adalah batas yang memisahkan antara TCB dengan faktor *reminder* dari sistem. Jalur terpercaya (*trusted path*) juga harus tersedia sehingga user dapat mengakses TCB tanpa harus kompromi dengan prosesor lain atau user lain. Sistem komputer yang terpercaya (*trusted computer system*) adalah sistem yang memakai ukuran jaminan hardware dan software untuk memungkinkan penggunaannya dalam memproses beberapa level klasifikasi atau informasi yang sensitif.

Konsep dari abstraksi (*abstraction*) yaitu melihat komponen sistem pada level tertinggi dan mengabaikan atau memisahkan detailnya. Pendekatan ini meningkatkan kapabilitas sistem untuk bisa mengerti sistem yang kompleks dan untuk berfokus pada hal-hal yang kritis dan *high-level*.

## 6.1 Rings

Satu skema yang mendukung beberapa proteksi domain adalah penggunaan ring proteksi.



**Gambar 1.5** Proteksi Ring

Keamanan sistem operasi kernal biasanya terdapat pada Ring 0 dan memiliki hak akses pada setiap domain di dalam sistem. Keamanan kernel didefinisikan sebagai hardware, firmware, dan software dari sebuah basis komputer yang terpercaya yang menerapkan konsep monitor referensi. Sebuah monitor referensi adalah sebuah komponen sistem yang melaksanakan kontrol akses pada sebuah objek.

Pada konsep ring ini, hak akses berkurang sejalan dengan lebih tingginya nomor ring. Sehingga proses yang paling terpercaya terdapat pada ring tengah. Mekanisme proteksi ring ini telah diimplementasi oleh sistem operasi *time-shared* MIT's MULTICS yang telah diperluas untuk mengamankan aplikasi.

Ada pula beberapa pendekatan proteksi berbasis kernel:

- Menggunakan peralatan hardware yang terpisah yang memvalidasi semua referensi dalam sebuah sistem.
- Mengimplementasi monitor mesin virtual, yang membangun sejumlah mesin visual yang tersembunyi satu dengan lainnya yang berjalan pada komputer.
- Menggunakan sebuah software kernel security yang mengoperasikan domain proteksi hardware miliknya sendiri.

## 6.2 Security Modes

Ada dua perbedaan cara dalam operasi sebuah sistem informasi yaitu *system high mode* dan *multi-level security mode*. Pada operasi *system high mode*, sebuah sistem beroperasi pada level tertinggi dari klasifikasi informasi. Sedangkan *multi-level*

*security mode* mendukung user yang memiliki perbedaan otorisasi dan data pada beberapa level klasifikasi. Beberapa tambahan mengenai cara operasi adalah:

- **Dedicated:** semua user memiliki otorisasi dan kebutuhan untuk mengetahui semua informasi yang diproses oleh sistem informasi. Sistem bisa menangani beberapa level klasifikasi.
- **Compartmented:** semua user memiliki otorisasi untuk level tertinggi dari klasifikasi informasi tetapi mereka tidak perlu untuk mengetahui semua informasi yang ditangani oleh sistem informasi.
- **Controlled.**
- **Limited access:** salah satu tipe dari akses sistem.

## BAB II MODEL KEAMANAN INFORMASI

Bentuk-bentuk yang digunakan dalam informasi keamanan memformalisasikan “Keamanan kebijakan”. Bentuk-bentuk keamanan ini bersifat abstrak atau intuisi dan melengkapi kerangka kerjanya untuk memahami konsep-konsep dasar. Pada bagian ini ada 3 bentuk yang akan dijelaskan, yaitu: Model kontrol akses, Model Integritas dan Modul Arus Informasi.

### 1. Access Control Models

Proses kontrol akses dapat dirangkai ke dalam bentuk yang membatasi ruang lingkup dasar dan perbedaan yang tampak pada model ini. Bentuk dari kontrol akses ini adalah akses matriks, model “Take-Grant”, Model “Bell-LaPadula”, dan model “State Machine” .

#### 1.1 The Access Matrix

Akses Matriks merupakan tindakan akses yang benar dirangkai dari subjek ke objek. Akses yang benar yaitu tipe data yang dapat membaca, menulis dan mengerjakan. Subjek merupakan kesatuan yang aktif untuk melakukan pencarian sumber atau objek yang benar. Subjek dapat berupa orang, program atau proses. Objek merupakan kesatuan yang pasif, seperti file atau tempat penyimpanan data. Dalam beberapa hal ini, satu sisi berupa subjek dalam konteks dan objek dalam konteks yang lainnya. Bentuk matriks kontrol akses ditunjukkan dalam tabel 2.1.

**Tabel 2.1 Contoh Matriks Akses**

Subjek/Objek	Data Masukan	Data Gaji	Proses Pengambilan	Print server A
Ad	Baca	Baca/Tulis	Bekerja	Tulis
Andi	Baca/Tulis	Baca	Tidak ada	Tulis
Proses Pengecekan	Baca	Baca	Bekerja	Tidak ada
Program Biaya	Baca/Tulis	Baca/Tulis	Panggil	Tulis

Kolom matriks akses disebut “Access Control Lists (ACLs)”, dan disebut “Capability Lists”. Bentuk matriks akses ini mendukung kontrol akses sepenuhnya karena matriks ini merupakan individu yang memiliki kendali sepenuhnya. Dalam matriks kontrol akses kemampuan subjek dibatasi oleh 3 macam bentuk (objek, posisi dan pengacakan). Jadi 3 bentuk yang membatasi ini posisi di mana subjek harus merupakan objek sepanjang pengacakan nomor berlangsung yang biasanya mencegah terjadinya proses pengulangan . Ketika bentuk batasan ini sama halnya

dengan “Karberos Tickets” yang dibahas pada bab sebelumnya “Sistem Kontrol Akses”.

Masalah yang paling penting dalam proteksi file adalah membuat akses yang bergantung pada identitas user yang mengakses berkas. Implementasi yang umum untuk menerapkan akses yang bergantung pada identitas sebuah file atau objek adalah Access Control List (ACL). ACL menspesifikasikan nama user dan tipe akses yang mana yang diizinkan untuk setiap user. Akan tetapi, terdapat kelemahan jika mengimplementasikan ACL untuk proteksi berkas:

1. Harus melist satu persatu user terhadap tipe akses yang diizinkan terhadap berkas.
2. Manajemen ruang kosong pada memori akan lebih susah.

Kelemahan ACL dapat diatasi dengan cara mengklasifikasikan user menjadi tiga, yaitu:

1. Owner, user yang membuat file/ objek tersebut.
2. Group, sekumpulan user yang berbagi file/ objek yang membutuhkan akses yang sama terhadap sebuah file/objek.
3. Universe, semua user pada sistem tersebut. Penulisannya adalah file/objek (owner, group, right).

Sebagai contoh, ada empat user (A, B, C, dan D) yang masing-masing termasuk dalam group system, staff, dan student.

File0 (A,\*, RWX)

File1 (A, system, RWX)

File2 (A, \*, RW-) (B, staff, R--) (D, \*, RW-)

File3 (\*, student, R--)

File4 (C,\*,---) (\*, student, R--)

File0 dapat dibaca, dieksekusi dan ditulis oleh user A pada semua group yang ada. File1 dapat dibaca, dieksekusi dan ditulis oleh user A pada group system. File2 dapat dibaca dan ditulis oleh user A dan D pada semua group, dibaca oleh user B pada group staff. File3 dapat dibaca oleh semua member dari group student. File4 memiliki keistimewaan yaitu ia mengatakan bahwa user C di setiap group tidak memiliki akses apapun, tetapi semua member group student dapat membacanya, dengan menggunakan ACL memungkinkan menjelaskan spesifik user, group yang mengakses sebuah file atau objek.

Kebanyakan sistem informasi bagi usaha kecil dan menengah dibangun dengan asumsi tidak terdapat keamanan komputer yang akan diterapkan. Kebutuhan tersebut cukup hingga kemajuan teknologi jaringan umumnya dan internet pada khususnya dan peningkatan penggunaan koneksi yang terus tersambung seperti xDSL dan model kabel. Koneksi ke internet yang selalu tersambungkan ini berarti komputer dapat diketahui dengan mudah oleh hacker, karena keberadaan komputer relatif lebih mudah diprediksi dan alamat IP yang stabil-yang berarti baik alamat IP

yang statis atau bentuk pool kecil alamat yang berdekatan. Jika alamat IP koneksi komputer pengguna ke internet statis, komputer tersebut cukup ditemukan satu kali saja; jika alamat IP koneksi komputer pengguna ke internet diberikan secara dinamis, hacker harus mencari tiap kali ingin mengetahui lokasi komputer tersebut tetapi sering kali pencarian tersebut hanya pada sejumlah kecil alamat dari koleksi alamat yang telah diketahui. Begitu sebuah komputer telah ditemukan alamatnya, cracker atau hacker dapat mulai mencari informasi atau menyerang komputer pengguna tersebut. Hal inilah yang menjelaskan mengapa saat pengguna komputer lebih sering terhubung ke internet, kebutuhan keamanan pengguna komputer tersebut juga meningkat.

Satu cara utama untuk memperoleh keamanan komputer adalah mengizinkan atau membatasi akses ke file atau directory atau sumber daya komputasi yang dipergunakan pengguna komputer pada suatu komputer. Dengan pembatasan akses tersebut, administrator komputer dapat mengetahui siapa yang atau yang tidak melakukan suatu aktifitas pada sistem yang diaturnya. Hal yang lebih penting, administrator dapat mengendalikannya siapa saja yang melakukan aktifitas tertentu.

Suatu usaha kecil menengah bisa memiliki roles acces controll sesuai kebutuhannya, tapi sebaiknya pengelompokan izinnya unik. Dan tidak ketinggalan pula, bahwa terlalu banyak role berarti memerlukan perawatan struktur keamanan yang lebih.

Untuk pemilihan sistem operasi pada usaha kecil dan menengah, sebaiknya menggunakan sistem operasi yang memiliki setting default sistem keamanan yang cukup. Hindari penggunaan windows9x dan windows ME, karena sistem operasi tersebut memiliki kemampuan yang terbatas dalam mengontrol dan mengelola pengguna.

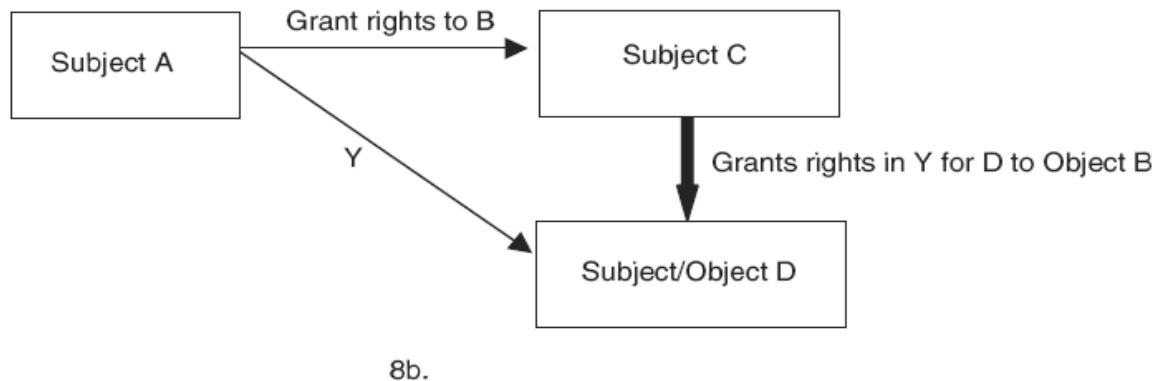
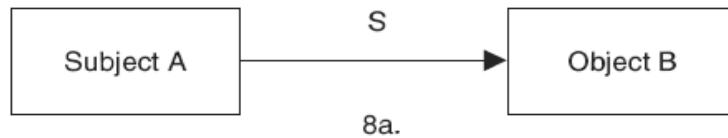
## 1.2 Take-Grant Model

Bentuk "Take-Grant" menggunakan petunjuk grafik untuk posisi yang lebih spesifik bahwa subjek dapat mentransfer objek dan sebuah subjek dapat diambil dari subjek lainnya. Contoh: Asumsikan bahwa Subjek A menduduki posisi yang mencakup posisi "Grant" yang ditujukan ke objek B. Kejadian ini digambarkan dalam gambar 2.2.8a. Kemudian asumsikan bahwa subjek A dapat mentransfer posisi "Grant" untuk objek B ke objek C, dan subjek A menempati posisi yang lain (Y) ke objek D. Dalam beberapa hal ini objek D berlaku sebagai sebuah objek dan objek lainnya berlaku sebagai subjek. Kemudian seperti yang ditunjukkan oleh panah tebal dalam gambar 2.2.8b, subjek C menempati posisi "Y" ke subjek/objek D, karena subjek A melewati posisi "Grant" ke subjek C.

"Take Capability" bekerja dalam bentuk khusus seperti gambar "Grant".

### 1.3 Bell-LaPadula Model

Bentuk Bell-LaPadulla dikembangkan untuk memformalkan kebijakan keamanan multi level Departemen Keamanan Amerika Serikat. Label DoD merupakan klasifikasi keamanan pada tingkatan yang berbeda. Seperti pada pembahasan sebelumnya, tingkatan ini terdiri dari “UnClasified”, “Confidential”, “Secret” dan “Top Secret” dari sensitivitas yang paling kecil ke sensitivitas yang paling besar.



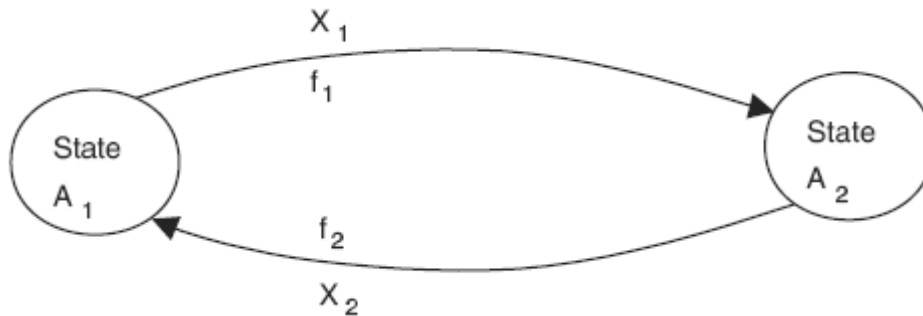
**Gambar 2.1. Model Take-Grant [RON05: 304]**

Individual yang menerima penjelasan “Confidential”, “Secret”, atau “top Secret” dapat mengakses material pada klasifikasi tingkatan tersebut atau di bawahnya. Syarat tambahan, bagaimanapun juga individual harus memiliki pengetahuan mengenai material tersebut. Jadi seorang individual menjelaskan “Secret” hanya dapat mengakses label data “secret” yang penting bagi individual guna menampilkan fungsi tugas pekerjaan. Bentuk Bell-LaPadulla setuju dengan penggolongan material. Bentuk Bell-LaPadulla tidak dialamatkan secara lengkap atau sempurna.

Model Bell-LaPadulla dengan konsep “State Machine”, konsep ini membatasi rangkaian kondisi yang diizinkan ( $A_i$ ) dalam sistem. Perpindahan dari satu tempat ke tempat lainnya di atas penerima input ( $X_i$ ) yang dibatasi oleh fungsi transisi ( $f_k$ ). Kenyataan model ini menjamin bahwa posisi awal merupakan kepastian dan bahwa transisi selalu berhasil. Perpindahan (transisi) antara 2 tempat digambarkan dalam gambar 2.2

Bentuk Bell-LaPadulla membatasi posisi yang telah ditetapkan melalui 3 unsur multi level yang pertama 2 unsur penerapan kontrol akses dan yang ketiga, 1 unsur yang diizinkan kontrol akses. Unsur-unsur dijelaskan sebagai berikut:

1. Unsur keamanan yang sederhana (unsur ss) menyatakan pembacaan informasi oleh subjek pada tingkatan sensitivitas yang lebih rendah dari objek tingkatan sensitivitas yang lebih tinggi yang tidak diizinkan (tidak terbaca).



**Gambar 2.2. Perpindahan Posisi Dibatasi Oleh Fungsi F Dan Input X. [RON05:305]**

2. Unsur keamanan bintang (\*), menyatakan penulisan informasi dengan subjek pada tingkatan sensitivitas yang lebih tinggi ke objek tingkatan yang lebih rendah tidak diizinkan tidak terbaca).
3. Unsur keamanan polisi. Menggunakan matriks akses untuk mengenal kode akses kontrol.

Kecepatan unsur bintang (\*) terlalu terbatas dan menambah data yang disyaratkan. Misalnya unsur ini dapat memindahkan paragraf yang sensitivitasnya lebih rendah dalam dokumen yang lebih tinggi ke dokumen yang sensitivitasnya lebih rendah. Transfer informasi diizinkan oleh bentuk Bell-LaPadulla melalui subjek yang dipercaya (trusted subject). Trusted Subject dapat melanggar unsur bintang (\*), namun sekarang tidak bisa lagi.

Dalam beberapa contoh, sebuah unsur yang disebut unsur yang keras ketetapanannya. Unsur ini menetapkan bahwa pembacaan dan penulisan yang diizinkan pada tingkatan sensitivitas tertentu tetapi tidak juga untuk tingkatan sensitivitas yang lebih tinggi atau lebih rendah.

Model ini membatasi permintaan sistem. Permintaan dibuat saat sistem dalam posisi  $v1$ ; sebuah keputusan ( $d$ ) dibuat di atas permintaan, dan sistem mengubah posisi  $v2(R,d,v1,v2)$  yang mewakili jenis model ini. Kadang-kadang kecepatan model (bentuk) ini memastikan bahwa ada perpindahan dari satu tempat (posisi) ke tempat yang lain.

Model kerja Bell-LaPadulla berdasarkan pada akses matriks. Sistem keamanan polisi membatasi pengendalian khusus ke sumber sistem. Pengendalian berhubungan dengan bagaimana posisi mengakses yang dibatasi dan bagaimana mereka mengevaluasi (mengecek). Beberapa pencapaian sistem kerja berdasarkan ketergantungan konteks dan kontrol akses ketergantungan isi. Ketergantungan isi mengontrol membuat keputusan akses berdasarkan data yang ada dalam objek, sebaliknya kontrol ketergantungan konteks menggunakan subjek atau atribut objek ataupun karakteristik sistem untuk membuat keputusan. Contoh beberapa karakteristik termasuk aturan kerja, akses-akses awal, dan pembuatan file tanggal dan waktu.

Karena banyak bentuknya, model Bell-LaPadulla memiliki kelemahan. Berikut ini salah satu kelemahannya yang besar adalah:



**Gambar 2.3. Biba Model Axioms [RON05: 306]**

- Model ini memungkinkan atau mengizinkan atau mempertimbangkan jalur perubahan informasi yang normal dan tidak memperbolehkan jalur yang tersembunyi atau rahasia
- Model ini tidak sejalan dengan sistem modern yang menggunakan pembagian arsip dan banyak pengelola (data)
- Model ini tidak secara gamblang atau tegas membatasi apa yang diinginkan dengan sebuah perubahan keadaan yang tertutup

- Model ini berdasarkan pada kebijakan pengamanan bertingkat atau berjenjang dan tidak memperbolehkan model jenis kebijakan lain yang mungkin digunakan oleh sebuah organisasi.

## 2. Integrity Models

Pada banyak organisasi baik pemerintahan maupun bisnis keterbukaan data adalah penting atau lebih penting dari pada kerahasiaan pada penerapan / aplikasi tertentu. Jadi model keterpaduan resmi dikembangkan, singkatnya model keterpaduan di kembangkan sebagai suatu perbandingan atas model kerahasiaan Bell-LaPadulla dan kemudian menjadi lebih mampu untuk menghadapi keperluan meningkatnya syarat penambahan keterpaduan.

### 2.1 The Biba Integrity Model

Keterpaduan ini biasanya dicirikan dengan 3 tujuan berikut :

1. Data dilindungi dari perubahan yang dibuat oleh para pengguna yang tidak berhak.
2. Data dilindungi dari modifikasi atau perubahan yang tidak di perkenankan oleh pengguna yang berhak.
3. Data ini pada bagian dalam dan bagian luar saling bersesuaian data yang didapat. Pada sumber data harus seimbang pada bagian dalam dan sesuai dengan bagian luar, situasi dunia nyata.

Untuk menuju sasaran keterpaduan pertama, model biba dikembangkan pada tahun 1977 sebagai perbandingan keterbukaan atas model kerahasiaan Bell-LaPadulla. Model biba berdasarkan pola-pola dan menggunakan hubungan kurang dari atau sama dengan. Pola-pola struktur ini diartikan sebagai kumpulan perintah terpisah dengan Least Upper Bound (LUB) : (batas yang lebih tinggi dari terendah) dan Greatest Lower Bound (GLB) : (batas yang lebih rendah dari yang tertinggi). Pola-pola ini mewakili sekumpulan tingkat keterpaduan dari suatu hubungan perintah yang termasuk dalam tingkatan tersebut.

Mirip dengan model klasifikasi tingkat perbedaan kepekaan Bell-LaPadulla model biba menggabungkan objek ke dalam tingkat perbedaan keterbukaan. Model ini menggolongkan 3 aksioma (ketetapan) keterpaduan :

1. Aksioma (ketetapan) keterbukaan sederhana.  
Menetapkan bahwa subjek pada sebuah tingkat keterpaduan tidak diperbolehkan untuk meneliti sebuah objek pada tingkat keterbukaan yang lebih rendah (tidak melihat ke bawah)
2. The \* (star) Integrity Axiom.  
Menetapkan bahwa sebuah objek pada suatu tingkat keterbukaan tidak diperbolehkan untuk mengubah suatu objek dari tingkat keterpaduan yang lebih tinggi.

3. Sebuah subjek dari level pertama keterpaduan tidak dapat meminta sebuah objek atas level / tingkatan keterpaduan yang lebih tinggi

## 2.2 The Clark-Wilson Integrity Model

Model pendekatan metode Clack - Wilson (1987) telah dikembangkan sebagai suatu kerangka kerja yang digunakan pada dunia nyata di lingkungan perniagaan / bisnis. Model ini merujuk pada 3 sasaran keterbukaan dan menegaskan syarat-syarat sebagai berikut :

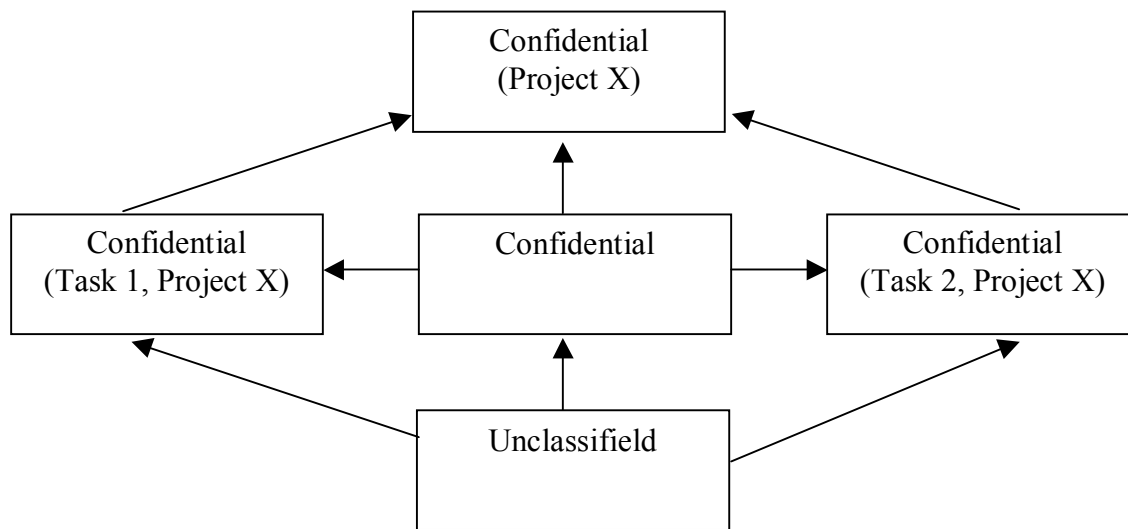
- Constrained Data Item (CDI) => bagian data yang mendesak  
Sebuah data pokok yang mempunyai keterpaduan sebagai sesuatu yang dipelihara
- Integrity Verification Prosedure (IVP) => Prosedur Pemeriksaan Keterpaduan  
Memperkuat semua hal tentang CDI yang merupakan sesuatu yang benar dari suatu wujud keterpaduan
- Transformation Prosedure (TP) => Prosedur Transformasi  
Manipulasi dari CDIs yang telah selesai yang merupakan suatu transaksi yang berbentuk baik. Yang mana telah ada perubahan CDI dari satu wujud keterbukaan ke wujud keterpaduan yang lainnya.
- Unconstrained Data Item => Sistem (bagian) yang tidak mendesak  
Bagian data ini terletak di bagian luar dari tempat kontrol (pengawasan\_ dari contoh lingkungan, sebagai contoh masukan informasi.

Model Clack – Wilson membutuhkan penamaan keterpaduan untuk memutuskan tingkatan keterpaduan dari sebuah bagian data untuk membuktikan bahwa keterpaduan ini telah terpelihara setelah menggunakan aplikasi dari suatu TP (Transformation Prosedure). Model ini telah memasukkan mekanisme dalam menjalankan data dari luar kemantapan dalam mengambil tindakan, pemisahan dari kewajiban dan keterpaduan kebijaksanaan oleh pemberi perintah.

## 3. Information Flow Models

Suatu model aliran informasi yang berdasarkan atas wujud mesin, dan aliran ini terdiri dari suatu objek, wujud peralihan dan pola-pola (kebijakan mengalir) keadaan. Pada keadaan seperti sekarang ini, objek juga bias mewakili penggunaannya, sebuah informasi yang memaksa untuk mengikuti aliran dalam suatu pengawasan yang harus memiliki surat izin oleh kebijakan keamanan. Sebagai contoh ditunjukkan pada gambar 2.4.

Dalam gambar 2.4 Aliran informasi dari sesuatu yang tidak digolongkan menjadi suatu rahasia di dalam tugas di proyek x dan kombinasi tugas di proyek x. Informasi ini dapat mengikuti aliran informasi di dalam satu aturan.



**Gambar 2.4 Model Alir Informasi [RON05: 309]**

### 3.1 Non-Interference Model

Model ini menceritakan tentang model aliran informasi dengan larangan yang terdapat pada aliran informasi. Pada dasarnya prinsip model ini adalah merupakan sebuah grup yang terdiri dari para pengguna (A). Seorang yang menggunakan Perintah (C). Jangan mencampuri urusan para pengguna (B), seseorang yang menggunakan perintah (D). Konsep ini ditulis sebagai  $A, C \vdash B, D$  Perintah untuk menyatakan kembali peraturan ini. Tindakan yang dilakukan oleh grup A yang menggunakan perintah C tidak dapat dilihat oleh para pengguna grup B yang menggunakan perintah D.

### 3.2 Composition Theories

Pada beberapa aplikasi, sistem ini dibangun oleh kombinasi sistem-sistem yang kecil. Sebuah situasi yang menarik perhatian untuk menanggapi apakah keamanan suatu komponen sistem telah mampu terpelihara ketika mereka akan mengkombinasikan ke dalam sebuah entitas formulir yang besar.

Jhon Mc Clean mempelajari tentang persoalan ini pada tahun 1994 (MCLean. J). “Teori keseluruhan tentang suatu komposisi yang digunakan untuk menetapkan jejak tertutup di bawah fungsi untuk disisipkan di antaranya”. Dimulai pada tahun 1994 IEEE kumpulan karangan penelitian tentang keamanan dan kerahasiaan IEEE Press, 1994)”

Dia mendefinisikan 2 buah gagasan komposional : yaitu dari dalam dan luar. Berikut ini adalah beberapa tipe gagasan yang berasal dari luar.

- Cascading, Suatu sistem masukan yang mendapatkan dari keluaran dari sistem yang lainnya.

- Feedback, Satu sistem yang memberikan masukan kepada sistem kedua, yang merupakan putaran arus balik yang berasal dari masukan pada sistem yang pertama.
- Hookup, Sebuah sistem yang merupakan kombinasi dengan sistem lainnya sebaik dengan entitas yang berasal dari luar.

Gagasan komposisi internal (dari dalam) adalah suatu titik potong, perpaduan dan perbedaan. Keseluruhan kesimpulan dari pelajaran ini adalah tentang keamanan kepemilikan dari suatu sistem yang kecil di mana telah terpelihara di bawah suatu komposisi (di beberapa instansi). Dalam gagasan cascading sebelumnya telah juga terdapat suatu subjek yang berasal dari variabel sistem yang berasal dari gagasan yang lainnya.

## **BAB III**

### **PENJAMINAN**

Assurance (Penjaminan) secara singkat adalah tingkat kepercayaan dalam kepuasan dari kebutuhan pengamanan.

#### **1. Kriteria Evaluasi**

Di tahun 1985, Trusted Computer System Evaluation Criteria (TCSEC) dikembangkan oleh National Computer Security Center (NCSC) untuk menyediakan panduan untuk evaluasi vendor produk untuk spesifikasi kriteria pengamanan. TCSEC menyediakan sebagai berikut:

- Dasar pembangunan kebutuhan pengamanan dalam
- Pelayanan pengamanan standar yang seharusnya disediakan oleh vendor- vendor untuk kelas- kelas kebutuhan pengamanan yang berbeda
- Sebuah usaha untuk mengukur tingkat kepercayaan dari sebuah sistem informasi.

Dokumen TCSEC disebut Orange Book dikarenakan warnanya, ini bagian dari seri panduan dengan cover yang berbeda warna yang disebut seri Rainbow. Dalam buku Orange, kontrol objektivitas dasar adalah polis pengamanan, penjaminan, dan accountability. TSCEC mencakup kepercayaan tapi tidak mencakup integritas. Juga secara fungsional (aplikasi kontrol pengamanan) dan penjaminan (kepercayaan bahwa sebuah sistem keamanan yang berfungsi sebagaimana mestinya) tidak terpisahkan dalam TSCEC seperti ada pada kriteria pengembangan evaluasi nantinya. Orange Book mendefinisikan kelas hierarki utama pengamanan dengan huruf D sampai A seperti berikut

- D Perlindungan minimal
- C Perlindungan Discretionary (C1 dan C2)
- B Perlindungan Mandatory (B1, B2, dan B3)
- A Perlindungan Verified; methods formal (A1)

DoD Trusted Network Interpretation (TNI) adalah analogi untuk Orange Book, yang dialamatkan secara konfidensial dan integritas dalam trusted computer/ sistem komunikasi jaringan dan disebut Red Book. Sistem Interpretasi Manajemen Database Trusted/ Trusted Database Management System Interpretation (TDI) mengalamatkan sistem manajemen database Trusted. European Information Technology Security Evaluation Criteria (ITSEC) mengalamatkan masalah C.I.A. Produk atau sistem yang dievaluasi ITSEC didefinisikan sebagai Target Evaluasi/ Target of Evaluation (TOE). TOE harus memiliki target pengamanan, yang termasuk mekanisme enforcing security dan kebijakan keamanan sistem.

ITSEC secara sebagian mengevaluasi fungsionalitas dan penjaminan, dan dimasukkan dalam 10 kelas fungsionalitas (F), 8 tingkat penjaminan (Q), 7 tingkat pemeriksaan (E), dan 8 dasar fungsi pengamanan dalam kriteria ini. ITSEC juga mendefinisikan dua jenis penjaminan. Satu, ukuran penjaminan dalam pemeriksaan implementasi fungsi pengamanan, dan yang lain efektivitas TOE saat pengoperasian.

Rating ITSEC dalam bentuk F-X, E, fungsionalitas dan penjaminan di-list. Rating ITSEC yang diekuivalen dengan rating TCSEC seperti berikut :

F-C1, E1 = C1

F-C2, E2 = C2

F-B1, E3 = B1

F-B2, E4 = B2

F-B3, E5 = B3

F-B3, E6 = A1

## **2. Sertifikasi dan Akreditasi**

Dalam beberapa lingkungan, method formal harus dapat diaplikasikan untuk menjamin pengamanan keamanan sistem informasi sudah ada dan berjalan sebagaimana mestinya untuk tiap spesifikasi. Sebagai tambahan, sebugah otoritas harus bertanggung jawab meletakkan sistem ke dalam pengoperasian. Aksinya dikenal sebagai sertifikasi dan akreditasi.

Secara formal, definisinya sebagai berikut:

Sertifikasi. Perbandingan evaluasi fitur pengamanan teknik dan non-teknik sistem informasi dan pengamanan yang lain, yang dibuat dalam mendukung proses akreditasi untuk membangun keberadaan dari desain dan implementasi tertentu yang akan cocok dengan spesifikasi kebutuhan pengamanan.

Akreditasi. Deklarasi formal dari Designated Approving Authority (DAA) dimana sistem informasi di-approve untuk mengoperasikan dalam mode sistem tertentu dengan menggunakan panduan keamanan yang telah dibuat sebelumnya dengan tingkat resiko yang dapat diterima.

Sertifikasi dan akreditasi sistem harus di-cek setelah mendefinisikan periode waktu atau saat merubah kejadian dalam sistem dan/ atau lingkungannya.

Kemudian, sertifikasi ulang dan akreditasi ulang dibutuhkan.

## **3. DITSCAP dan NIACAP**

Dua standard sertifikasi pertahanan dan pemerintah telah dikembangkan untuk evaluasi sistem informasi yang kritis. Standar ini adalah Defense Information Technology Security Certification and Accreditation Process (DITSCAP) dan the National Information Assurance Certification and Accreditation Process (NIACAP).

### **3.1 DITSCAP**

DITSCAP membuat proses standar, satu set aktivitas, deskripsi tugas umum, dan struktur manajemen untuk mensertifikasi dan mengakreditasi sistem IT yang akan menjaga bentuk pengamanan yang dibutuhkan. Proses ini didesain untuk mensertifikasi sistem IT yang cocok dengan kebutuhan akreditasi dan sistem akan tetap mengakreditasikan keamanannya selama proses siklus.

Berikut empat fase untuk DITSCAP:

**Fase 1, Definisi.** Fase 1 terfokus pada pengertian misi, lingkungan dan arsitektur dalam rangka menentukan kebutuhan pengamanan dan tingkat usaha yang diperlukan untuk menghasilkan akreditasi

**Fase 2, Verifikasi.** Fase 2 memverifikasi mencakup atau modifikasi sistem yang compliance dengan informasi yang disetujui dalam System Security Authorization Agreement (SSAA). Tujuan digunakan SSAA untuk membangun sebuah kesepakatan yang sebelumnya disetujui untuk menentukan tingkat keamanan yang dibutuhkan sebelum pengembangan sistem mulai atau berubah ke sistem yang dibuat. Setelah akreditasi, SSAA menjadi dasare pengamanan konfigurasi dokumen.

**Fase 3, Validasi.** Fase 3 memvalidasi compliance dari sistem yang terintegrasi secara keseluruhan dengan pusat informasi dalam SSAA.

**Fase 4, Post Akreditasi.** Fase 4 meliputi aktivitas yang diperlukan untuk melanjutkan operasi akreditasi sistem IT dalam lingkungan komputasinya dan pengalamanan perubahan masalah tampilan sistem yang melalui life cycle.

### 3.2 NIACAP

NIACAP membangun standar nasional minimum untuk sertifikasi dan akreditasi sistem pengamanan nasional. Proses ini menyediakan set standar aktivitas, tugas umum, dan struktur manajemen untuk mensertifikasi dan mengakreditasi sistem yang menjaga informasi penjaminan dan pengamanan bentuk sistem atau site.

NIACAP dibuat dari empat fase: Definisi, Verifikasi, Validasi dan Post Akreditasi. Fase – fase ini secara inti mirip dengan DITSCAP. Sekarang, Commercial Information Security Analysis Process (CIAP) sedang dibangun untuk evaluasi sistem informasi yang sangat kritis dengan menggunakan metodologi NIACAP.

### 3.3 Systems Security Engineering - Capability Maturity Model (SSE-CMM)

Systems Security Engineering Capability Maturity Model (SSE-CMM, memiliki hak cipta tahun 1999 oleh Systems Security Engineering Capability Maturity Model [SSE-CMM] Project) berdasarkan asumsi yang jika anda bisa menjamin kualitas produk dan service yang dihasilkan oleh proses itu. Ini dikembangkan oleh consortium pemerintah dan ahli industri dan sekarang di bawah auspices International Systems Security Engineering Association (ISSEA) di [www.issea.org](http://www.issea.org). SSE-CMM memiliki salient point seperti berikut :

- Mendeskripsikan karakteristik essensial proses teknik pengamanan untuk menjamin teknik pengamanan yang baik.
- Mendapatkan praktek- praktek industri terbaik
- Menyetujui cara pendefinisian praktek dan peningkatan kemampuan.
- Menyediakan pengukuran perkembangan kemampuan proses aplikasi.

SSE-CMM mengalami area pengamanan berikut:

- Pengamanan Operasional
- Pengamanan Informasi
- Pengamanan Jaringan

- Pengamanan Fisik
- Pengamanan Personil
- Pengamanan Administratif
- Pengamanan Komunikasi
- Pengamanan Emanasi
- Pengamanan Komputer

Metodologi dan metrics SSE-CMM menyediakan pilihan untuk membandingkan sistem yang sekarang dengan sistem yang penting dalam elemen yang dijelaskan dalam model. SSE-CMM mendefinisikan dua dimensi yang digunakan untuk mengukur kemampuan organisasi untuk membentuk aktivitas yang spesifik. Dimensinya adalah domain dan kemampuan. Dimensi domain berisi seluruh praktek yang secara kolektif mendefinisikan teknik pengamanan. Praktek ini disebut Base Practices (BPs). Hubungan BPs digabungkan ke dalam Process Areas (PAs). Dimensi Capability menghadirkan praktek- praktek yang mengindikasikan manajemen proses dan kemampuan institusionalisasi.

Praktek ini disebut Generic Practices (GPs), karena mereka diaplikasikan di domain yang sangat luas. GP merepresentasikan aktivitas yang harus dilakukan sebagai bagian dari tindakan dalam melakukan BPs.

Untuk dimensi domain, SSE-CMM menspesifikasi 11 teknik pengamanan PAs dan 11 organisasi dan project yang berhubungan dengan PAs, masing- masing berisi BPs. BPs merupakan karakteristik utama yang harus ada dalam implementasi proses rekayasa keamanan sebelum sebuah organisasi mengklaim telah masuk dalam PA tertentu. PAs adalah sebagai berikut:

#### SECURITY ENGINEERING

- PA01 Administer Security Controls
- PA02 Assess Impact
- PA03 Assess Security Risk
- PA04 Assess Threat
- PA05 Assess Vulnerability
- PA06 Build Assurance Argument
- PA07 Coordinate Security
- PA08 Monitor Security Posture
- PA09 Provide Security Input
- PA10 Specify Security Needs
- PA11 Verify and Validate Security

#### PROJECT AND ORGANIZATIONAL PRACTICES

- PA12.Ensure Quality
- PA13.Manage Configuration
- PA14.Manage Project Risk
- PA15.Monitor and Control Technical Effort
- PA16.Plan Technical Effort

- PA17. Define Organization's Systems Engineering Process
- PA18. Improve Organization's Systems Engineering Process
- PA19. Manage Product Line Evolution
- PA20. Manage Systems Engineering Support Environment
- PA21. Provide Ongoing Skills and Knowledge
- PA22. Coordinate with Suppliers

GP diurutkan dalam tingkat kematangan dan di kelompokkan untuk membentuk dan membedakan diantara kelima tingkat kematangan rekayasa keamanan. Atribut – atribut adalah sebagai berikut:

- Level 1
  - 1.1 BPs Are Performed
- Level 2
  - 2.1 Planning Performance
  - 2.2 Disciplined Performance
  - 2.3 Verifying Performance
  - 2.4 Tracking Performance
- Level 3
  - 3.1 Defining a Standard Process
  - 3.2 Perform the Defined Process
  - 3.3 Coordinate the Process
- Level 4
  - 4.1 Establishing Measurable Quality Goals
  - 4.2 Objectively Managing Performance
- Level 5
  - 5.1 Improving Organizational Capability
  - 5.2 Improving Process Effectiveness

Penjelasan atas kelima level diatas adalah sebagai berikut :

- Level 1, “ Dilakukan secara informal, “ fokus pada organisasi atau proyek yang melakukan suatu proses yang melibatkan BP. Pernyataan khusus untuk level ini adalah. “Anda harus melakukannya sebelum anda bisa mengaturnya”.
- Level 2, “Direncanakan dan DiTrack”, fokus pada definisi level-proyek, perencanaan dan isu-isu performance. Pernyataan yang sesuai untuk karakter level ini, “Pahami apa yang terjadi pada suatu proyek sebelum menjelaskan proses yang lebih mendalam.
- Level 3, “Dilakukan dengan baik”, fokus pada bidang pekerjaan dari proses yang dijelaskan pada level organisasi. Pernyataan yang sesuai untuk level ini adalah :Gunakan yang terbaik apa yang telah anda pelajari dari proyek-proyek anda untuk menghaikasn proses yang lebih baik.

- Level 4, “Secara Kuantitatif Terkontrol”, fokus pada pengukuran yang diikat pada hasil bisnis pada suatu organisasi. Meskipun penting untuk memulai pengumpulan dan menggunakan ukuran poyek mendasar sejak awal, pengukuran dan penggunaan data yang tidak diharapkan sampai level yang lebih tinggi telah tercapai. Pernyataan khusus pada level ini “ Anda tak dapat mengukur sesuatu sampai anda tahu sesuatu itu apa dan “pengaturan dengan pengukuran hanya berarti pada saat anda mengukur hal-hal yang benar”.
- Level 5, “Improvisasi yang berkelanjutan”, mencapai pengaruh kekuatan dari keseluruhan kemajuan praktek manajemen yang terlihat pda level-level sebelumnya yang menekankan daya kultural yang akan menopang hasil yang diperoleh. Sebuah pernyataan yang memberikan makna khusus pada level ini adalah “sebuah budaya pengembangan yang berkesinambungan membutuhkan sebuah pondasi praktek manajemen, proses yang jelas dan hasil yang terukur”.

## **BAB IV**

### **IMPLEMENTASI CONTOH KASUS PADA UKM**

Dalam contoh kasus implementasi domain permasalahan ini, akan diambil sebuah UKM yaitu Cyber Campus Jakarta.

#### **1. Latar Belakang**

Cyber Campus didirikan pada bulan 01 Juni 2000 dengan tujuan untuk mentransformasi sistem pengetahuan dibidang Teknologi Informasi, sistem peluang pengembangan profesionalisme melalui peningkatan skill di bidang Teknologi Informasi, serta menyiapkan tenaga kerja yang handal bagi perusahaan-perusahaan dalam menghadapi AFTA.

Untuk menghadapi tantangan ini maka Cyber Campus memiliki rasa tanggung jawab yang sangat besar untuk dapat meningkatkan kemampuan sumber daya manusia yang ada saat ini. Cyber Campus berusaha untuk dapat meningkatkan mutu pendidikan dengan membuat kurikulum yang dapat dengan mudah mentransfer ilmu-ilmu yang dibutuhkan dalam pengembangan Teknologi Informasi dimana pendidikan Teknologi Informasi ini juga harus diimbangi dengan penyediaan sarana pendidikan yang berkualitas dan memadai. Seperti yang kita ketahui bahwa pendidikan bidang Teknologi Informasi memerlukan biaya yang tidak sedikit oleh karena itu masih sedikit sekali orang-orang yang bisa menikmati pendidikan di bidang ini. Dengan demikian, diperlukan dana yang cukup besar untuk mewujudkan SDM yang berkualitas dan mampu bersaing dalam bidang Teknologi Informasi.

Cyber Campus menyediakan program-program pendidikan yang mengupas habis tentang teknologi e-commerce. Cyber Campus menawarkan program profesional yang dapat menjadikan masyarakat menjadi seorang **Profesional TI**. Program Cyber Campus terdiri dari 3 jenis yaitu:

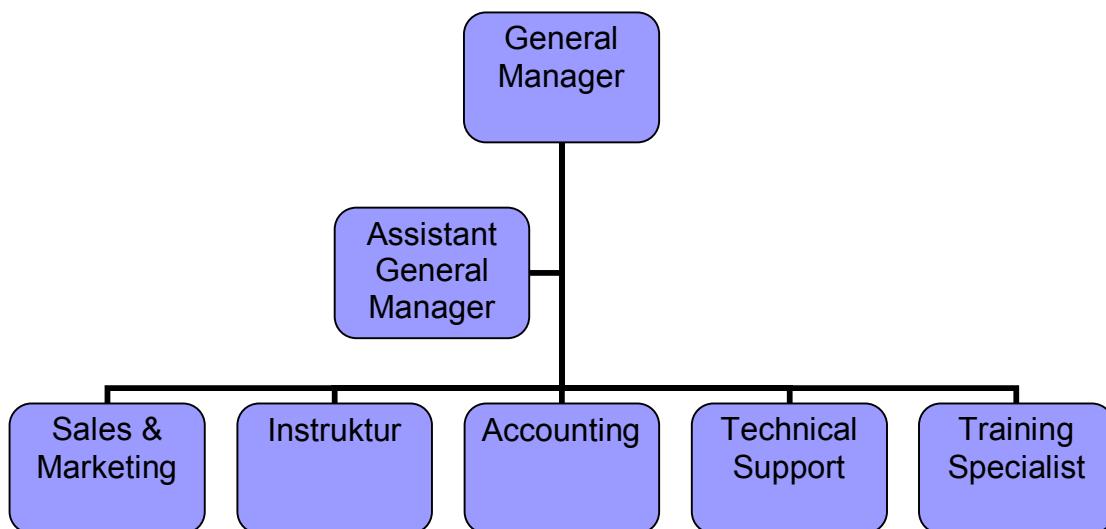
- Professional Cyber Expert (Program Profesi 1 tahun)
- Short Programs (1 bulan) :
  - WEB PROGRAMMER
  - WEB DEVELOPER
  - WEB DESIGN
  - Professional Class for Database
  - Professional VB Developer dll
- Special Application Training
  - WAP Database Application
  - Java mobile (J2ME) Application Training

Seluruh materi disampaikan dalam Bahasa Indonesia. Hal ini dimaksudkan agar setiap siswa dapat lebih cepat memahami dan menguasai materi yang dipelajari. Setiap materi telah dirancang sedemikian rupa agar dapat membuat siswa menjadi ahli pada bidang Teknologi Informasi.

Untuk memudahkan siswa yang berkualitas, setiap siswa akan ditantang dengan rancangan kasus-kasus latihan mandiri yang kami berikan melalui Program Interaktif. Program ini akan memberikan motivasi untuk melatih kemampuan siswa dalam menyelesaikan setiap kasus yang diberikan dengan metoda belajar profesional (lihat Metode Belajar).

Seiring dengan semakin matangnya usia Cyber Campus dalam penyelenggaraan dan bimbingan konsultasi IT kepada siswanya, Cyber Campus mulai melebarkan sayapnya dalam pembangunan dan pengembangan aplikasi sistem informasi. Pembangunan dan pengembangan sistem informasi ini ditujukan untuk dapat menambah keuntungan secara umum terhadap proses bisnis ataupun aktifitas instansi, perusahaan, badan usaha, ataupun pribadi. Dengan penggunaan IT dan sistem informasi yang handal diharapkan proses bisnis ataupun aktifitas sehari-hari yang *cheaper*, *better* dan *faster* dapat diwujudkan.

## 2. Struktur Organisasi Cyber Campus



Gambar 4.1 Struktur Organisasi Cyber Campus

**Tabel 4.1 Daftar Nama dan Jabatan**

No.	Nama	Jabatan
1	A01	<b>GENERAL MANAGER</b>
2	A02	Assisstant General Manager
3	A03	Sales & Marketing
4	A04 .. A06	Instruktur
5	A07	Accounting
6	A08	Technical Support
7	A09	Training Specialist

### 3. Aplikasi yang digunakan

Pada saat ini aplikasi yang digunakan untuk kegiatan sehari – hari / operasional perusahaan seperti pendaftaran, keuangan dan laporan adalah sebagai berikut:

- Aplikasi Data Keuangan : Zahir Accounting
- Data Pendaftaran : Microsoft Excel
- Data Laporan : Microsoft Word
- Sistem Operasi :
  - Client : Microsoft Windows 2000 Professional
  - Server : Microsoft Windows 2000 Server

### 4. Sistem Kontrol Akses

Dalam menganalisis keamanan yang ada disuatu organisasi atau perusahaan maka berdasarkan *orange book*, ada beberapa level mulai dari level A yang dikenal sebagai level tertinggi (*verified protection*) hingga level D (*minimal security*). Untuk mengetahui level suatu sistem dapat dilakukan dengan justifikasi. Keamanan level C dapat dijustifikasi sebagai berikut:

Justifikasi:

- o bila keamanan diserahkan ke sistem = level C2
- o bila keamanan diserahkan ke admin = level C1

Level sekuriti dari Cyber Campus termasuk C1, karena bila dilihat dari justifikasi diatas maka keamanan sistem dan jaringan diserahkan kepada admin (petugas administrator sistem dan jaringan komputer) yang akan mengelola sistem keamanan dengan pembatasan hak akses yang berbeda untuk tiap divisi yang ada di perusahaan.

Dalam rangka implementasi dari sistem kontrol akses yang dipergunakan di Cyber Campus adalah Access Control Matrix.

Akses kontrol adalah jantung dari keamanan. Akses kontrol adalah :

- Kemampuan untuk mengijinkan hanya kepada pengguna yang berhak

- Memberikan atau tidak memberikan hak akses, sesuai dengan model keamanan tertentu, dengan izin tertentu untuk mengakses suatu sumber informasi
- Seperangkat prosedur yang diterapkan pada perangkat keras, perangkat lunak dan administrator untuk memonitor akses, mengidentifikasi pengguna, mencatat akses yang telah dilakukan dan memberikan atau menolak akses berdasarkan peraturan yang telah dibuat.

Kontrol diimplementasikan untuk mengurangi resiko dan potensial kerugian. Kontrol dapat berupa :

- Preventif : mencegah terjadinya insiden
- Detektif : mendeteksi terjadinya insiden
- Korektif : memperbaiki terjadinya insiden

Untuk identifikasi dan otentikasi yang diterapkan pada Cyber Campus, digunakan nama login dan password. Setiap pengguna pada komputer , wajib memasukkan nama login dan password.

Kebijakan keamanan pada login yaitu :

- Minimal terdapat dua nama login pada setiap komputer klien. Satu nama login administrator dan satu nama login pengguna.
- Nama login pengguna masuk dalam kelompok pengguna (bukan administrator)
- Nama login tidak boleh diberikan kepada orang lain
- Apabila karyawan ataupun siswa sudah tidak menjadi anggota dari Cyber Campus, maka nama login-nya akan dihapus

Kebijakan pada password yaitu :

- Password paling sedikit terdiri dari delapan karakter tanpa spasi.
- Password merupakan kombinasi angka dan huruf
- Password pengguna diberikan oleh petugas sales dan marketing di lembar tertutup, dimana password tersebut dibuat oleh petugas technical support, dan haruslah diganti pada saat pertama kali login.
- Password haruslah diingat dan tidak boleh dicatat
- Password tidak boleh sesuatu yang mudah ditebak, seperti nama keluarga, tanggal lahir dan lain sebagainya.
- Password tidak boleh diberikan kepada orang lain

Kontrol akses pada file yang tersimpan pada komputer :

1. Setiap pengguna komputer mempunyai nama login yang unik. Setiap pengguna hanya boleh menyimpan pada “my documents” dari pengguna, dan tidak diperkenankan untuk mencoba membuka file selain dari folder tersebut.
2. Login pengguna dibatasi hanya dapat membuka file pada folder “my documents”. Pengguna dibatasi untuk tidak dapat meng-*install* program pada komputer.
3. Apabila pengguna memerlukan tambahan aplikasi perangkat lunak selain yang telah di-*install*, maka pengguna harus menghubungi petugas Technical Support.
4. Setiap user diperkenankan untuk berhubungan dengan internet

5. Setiap pengguna dapat memiliki nama login pada server data.
6. Terdapat direktori untuk semua divisi pada server. Hak akses pada file-file tersebut diberikan oleh pemilik informasi.
7. Hak akses untuk group dan untuk umum. Baik untuk group dan untuk umum, hak akses tersebut terbagi tiga yaitu melihat, mengedit dan mengeksekusi.
8. Dalam server Windows, petugas Technical Support membuat nama login dan memasukkan nama login tersebut dalam sebuah grup yang berhubungan dengan grup orang tersebut.

Untuk memformalkan kebijakan keamanan dalam organisasi, Cyber Campus menggunakan *Access Control Matrix Model*, yang menentukan apa yang boleh dan yang tidak boleh diakses oleh *user*. Sistem informasi pada Cyber Campus merupakan sistem yang terbuka yang dapat diakses dari luar Cyber Campus

*Access Control Matrix Model* untuk aset logikal yang terdapat dalam aplikasi – aplikasi yang ada di Cyber Campus.

**Tabel 4.2 Tabel *Access Control Matrix Model* Aplikasi Aset Logical**

User	Aplikasi Keuangan	Data Pendaftaran	Data Report	Sistem Operasi Client	Sistem Operasi Server	Data Server
A01	R	R	R	R/W*	-	R/W*
A02	R	R	R	R/W*	-	R/W*
A03	-	R/W	R/W	R/W*	-	R/W*
A04 .. A06	-	-	-	R/W*	-	R/W*
A07	R/W	R	-	R/W*	-	R/W*
A08	-	-	-	R/W	R/W	R/W*
A09	-	-	-	R/W*	-	R/W*
Siswa	-	-	-	R/W*	-	R/W*

Ket:

R = Read

W = Baca

- = Tidak mempunyai hak

R/W = Baca dan/atau Tulis

R/W\* = Baca dan/atau Tulis tapi terbatas haknya.

*Access Control Matrix Model* untuk aset fisik peralatan TI lainnya dapat dilihat pada tabel di bawah ini.

**Tabel 4.3 Tabel Access Control Matrix Model aset fisik peralatan TI**

User	PC	Server	Internet	Telepon & Faks	Printer
A01	X	-	X	X	X
A02	X	-	X	*	X
A03	X	-	X	X	X
A04 .. A06	X	-	X	-	X
A07	X	-	X	*	X
A08	X	X	X	-	X
A09	X	-	X	-	X
Siswa	X	-	X	-	-

Ket:

- X = Boleh Menggunakan
- = Tidak boleh menggunakan
- \* = Terbatas penggunaannya

Kontrol akses pada aplikasi :

1. Pada Aplikasi Keuangan, hanya staf accounting yang mempunyai akses untuk membaca dan menulis selain itu tidak memiliki akses.
2. Pada aplikasi pendaftaran, hanya staf sales dan marketing yang mempunyai akses menulis dan membaca, selain itu general manager hanya mempunyai hak membaca.
3. Pada aplikasi laporan, hanya staf sales dan marketing yang mempunyai akses menulis dan membaca selain itu tidak mempunyai akses baik membaca ataupun menulis.

### **Monitoring Kontrol Akses**

Untuk memonitor kontrol akses ini, hal-hal yang dapat dilakukan yaitu :

1. Technical Support akan mengecek setiap komputer 2 minggu sekali. Dalam pengecekan ini akan dilakukan pengecekan anti virus dan nama login serta hak ases terhadap setiap nama login. Apabila ditemukan nama login yang lain atau terdapat perubahan hak akses, maka kejadian ini Technical Support dapat melakukan informasi yang diperlukan.
2. Pemilik informasi berkewajiban untuk selalu mengecek hak akses pada setiap informasi yang dimiliki.
3. Setiap bulan sekali terdapat full backup data. Backup data ini tersimpan dalam kaset, yang tersimpan pada manajer Teknologi Informasi. Backup data ini bertahan sampai 3 tahun.
4. Apabila terjadi kecurigaan terhadap integritas data, maka dengan seijin pemilik data, petugas teknologi informasi dapat merestorasi informasi yang diinginkan.

### **Kepedulian Pada Keamanan**

Kepedulian pada keamanan (*security awareness*) harus ditumbuh kembangkan. Untuk itu perlu diadakan pelatihan internal maupun eksternal. Pelatihan ini ditujukan pada pegawai, administrator (divisi teknologi informasi), direktur dan petugas keamanan.

Hal-hal yang ditekankan pada kepedulian keamanan yaitu :

1. Informasi tidak dapat dijaga tanpa dukungan dari seluruh karyawan.
2. Pelatihan dapat dilaksanakan pada kelas ataupun penyebaran artikel.
3. Karyawan harus diajarkan pentingnya keamanan pada perusahaan dan bagaimana untuk mengidentifikasi dan melindungi informasi yang sensitif. Karyawan harus diberikan informasi mengenai kebijakan perusahaan dan ancaman dari lingkungan.
4. Administrator haruslah dilatih teknik keamanan yang terbaru, ancaman dan penanggulangannya.
5. Tanpa adanya dukungan dari pihak manajemen, program keamanan tidak dapat dijalankan.
6. Mempresentasikan secara berkala kepada pihak manajemen agar mereka selalu terinformasi status keamanan dari perusahaan.
7. Petugas sekuriti haruslah selalu tetap memberikan yang terbaik kepada perusahaan.
8. Kepada pihak manajer ditekankan bahwa keamanan bukan hanya masalah teknologi, tetapi juga masalah manusia.
9. Manajemen haruslah berusaha untuk menghindari konflik-konflik yang dapat mengakibatkan karyawan yang loyal menjadi seseorang yang dapat menyabotase sistem informasi.

### **Kebijakan Keamanan jaringan**

Kebijakan keamanan jaringan yang diterapkan pada Cyber Campus adalah sebagai berikut:

1. Instalasi software hanya boleh dilakukan oleh karyawan Technical Support
2. Sistem operasi yang digunakan oleh client adalah windows 2000 professional.
3. Setiap komputer harus di-*install* antivirus. Antivirus yang digunakan McAfee Anti-virus.
4. Setiap Network tidak saling berhubungan, kecuali ke Network sentral data dimana diletakkan sebuah Windows server sebagai sentral data.
5. Setiap *user* tidak dibenarkan memberikan *login account* kepada orang lain. Dan bertanggung jawab terhadap *login account* tersebut.
6. Setiap komputer dapat terhubung ke internet melalui firewall ADSL
7. Internet hanya digunakan untuk keperluan kantor, dan tidak boleh mengakses situs porno dan yang berhubungan dengan *crack* atau *hack*. Hal ini disebabkan situs-situs tersebut tidak berhubungan dengan keperluan perusahaan dan banyak virus bersumber pada situs-situs tersebut

8. Petugas Technical Support harus membatasi akses-akses ke internet dengan memblokir situs yang berhubungan dengan pornografi, *crack* dan *hack*. Pada saat ini dibatasi pada modem/firewall ADSL.
9. Pengguna tidak diperbolehkan mengubah setting keamanan pada sistem operasi, membuat *user account*, menggunakan perangkat untuk *crack / hack*, dan tindakan-tindakan yang dapat mengandung unsur kejahatan (misal, pencurian data, *scan IP*, *sniffing*).
10. Konfigurasi berbentuk Star, untuk itu perusahaan mempunyai ADSL modem/router/firewall cadangan yang akan dipergunakan bila alat tersebut rusak.
11. Perusahaan mempunyai cadangan HUB bila hub yang dipergunakan rusak.
12. Apabila memungkinkan Dapat pula dipasang Intrusion Detection System pada setiap Network.
13. Agar lebih efisien, web site Cyber Campus diletakkan pada web hosting sehingga pemeliharaan diserahkan pada perusahaan web hosting.
14. Sistem jaringan dibuat sentralisasi, PABX, ADSL modem, Windows server data dan semua HUB diletakkan pada ruang server
15. Setiap karyawan yang meninggalkan komputer haruslah *me-lock* komputer agar tidak dipergunakan oleh orang lain,
16. Setiap penanganan kerusakan, instalasi perangkat lunak, instalasi perangkat keras diharuskan mengisi log book.
17. Seluruh penyalahgunaan wewenang menjadi tanggung jawab pemegang otoritas.

### **Penentuan Tingkat Keamanan**

Dokumen-dokumen dalam lingkungan Cyber Campus dilakukan dengan menggunakan asas keamanan yang tinggi. Dokumen tersebut tidak boleh dibaca atau jatuh ke tangan karyawan yang tidak berkompeten apalagi pihak luar. Dengan demikian dibutuhkan

suatu mekanisme yang mengatur siapa yang berhak menggunakan dan siapa yang tidak dalam perusahaan.

Adanya pekerjaan atau proyek, pekerja, alat dan dokumen-dokumen dalam perusahaan menjadi pemikiran tersendiri bagi pendiri perusahaan untuk mengatur hubungan antar elemen tersebut. Aturan tersebut bisa kita sebut dengan aturan keamanan ataupun aturan pemakaian. Setiap sub elemen dari 4 elemen diatas harus diberikan batas yang jelas dari tugas dan wewenang masing-masing. Untuk itulah manajemen berusaha membuat sebuah policy keamanan untuk memenuhi kebutuhan tersebut.

Dengan security policy tersebut lebih lanjut bisa diharapkan kontinuitas dari perusahaan bila hal-hal yang tidak diinginkan terjadi. Dengan sendirinya policy tersebut akan memberikan garis yang jelas pada masing-masing elemen untuk lebih diberdaya gunakan secara optimal. Lebih lanjut policy tersebut akan membantu perusahaan menentukan hal-hal terbaik yang harus dilakukan setiap saat.

Penentuan tingkat keamanan dari sistem Cyber Campus berdasarkan pada kebutuhan akan sensitifitas data yang terdapat pada sistem informasi Cyber Campus dan kemampuan proses dari sistem tersebut. Masing-masing manager bertanggung

jawab akan penentuan tingkat keamanan sistem. Penentuan tingkat keamanan tersebut harus mempertimbangkan:

- Confidentiality, sistem berisikan informasi yang membutuhkan keamanan akses dari yang tidak berhak.
- Integrity, sistem berisi informasi yang harus dilindungi dari yang tidak berhak dan tidak diantisipasi, dan modifikasi oleh yang tidak berhak.
- Availability, sistem berisi informasi atau menyediakan layanan yang mesti tersedia ketika dibutuhkan

Setiap manager harus memastikan bahwa aplikasi digunakan oleh orang-orang yang memiliki otorisasi dengan tingkat keamanan yang telah ditetapkan dengan sebaik-baiknya. Penentuan tingkat keamanan tergantung berdasarkan 3 level sensitifitas dan 3 tingkat kritis. Semakin tinggi tingkat keamanan yang ditetapkan semakin tinggi kebutuhan akan keamanan.

**a. Tingkat Sensitifitas Data**

Penentuan tingkat sensitifitas data ini tergantung pada tipe data yang akan diakses dan peraturan baik perusahaan maupun negara yang harus dipenuhi. Adapun tingkat sensitifitas yang ditetapkan adalah sebagai berikut:

1. Tingkat sensitifitas rendah, dimana data yang diakses hanya membutuhkan tingkat keamanan yang rendah. Ancaman terhadap data cukup minimum dan minimal perhatian pengamanan dibutuhkan.
2. Tingkat sensitifitas moderat, dimana data yang diakses beberapa diantaranya penting bagi perusahaan dan membutuhkan cukup perhatian keamanan.
3. Tingkat sensitifitas tinggi, dimana data yang diakses memiliki banyak rahasia dimana kehilangan data ini akan berdampak cukup serius bagi perusahaan.

**b. Tingkat Kritis Data**

Tingkat kritis ini ditetapkan dalam penilaian proses yang termasuk kritis dan membutuhkan tingkat keamanan tertentu. Adapun tingkat kritis tersebut ditetapkan sebagai berikut:

1. Tingkat kritis rendah, proses yang teridentifikasi memiliki tingkat kritis yang rendah memerlukan pengamanan yang cukup dengan prioritas rendah.
2. Tingkat kritis moderat, proses yang teridentifikasi dipertimbangkan penting tapi tidak kritis untuk manajemen internal dari perusahaan.
3. Tingkat kritis tinggi, proses yang teridentifikasi kritis bagi perusahaan.

**Policy Keamanan Untuk Masing-Masing Elemen Dalam Struktur Organisasi**

**a. General Manager (A01)**

- Yang diperbolehkan :
  - Melakukan semua request terhadap informasi dari semua departemen yang ada
  - Melakukan login jaringan sebagai superuser (akses terhadap semua aplikasi )
  - Memperoleh Internet akses

- Memperoleh email akses
- Mengakses share direktori server
- Memperoleh direct line telepon
- Memegang kunci ruangan direktur
- Yang tidak diperbolehkan :
  - Menghapus data dalam jaringan komputer tanpa persetujuan dari pemilik atau pembuat

Penjelasan :

Dalam hal ini seorang general manager diberi akses untuk semua perangkat lunak, perangkat keras dan pegawai. Semua akses tersebut bisa sangat berguna atau membantu dalam pengambilan keputusan yang berakibat pada berjalannya perusahaan. Dengan berjalannya roda perusahaan tersebut secara langsung akan memberikan pengaruh positif pada karyawan yang dipimpin. Dengan kinerja yang meningkat diharapkan karyawan mampu memberikan segala daya upayanya untuk perusahaan.

**b. Ass. General Manager (A02)**

- Yang diperbolehkan :
  - Melakukan login ke jaringan sebagai user
  - Mengakses perangkat lunak aplikasi – aplikasi perkantoran
  - Memperoleh internet akses
  - Memperoleh email akses
  - Mengakses share direktori server
- Yang tidak diperbolehkan :
  - Menghapus data tanpa persetujuan pembuat data dalam share direktori
  - Memberikan hak akses terhadap softcopy dan hardcopy dokumen pada user dari luar perusahaan

**c. Sales & Marketing (A03)**

- Yang diperbolehkan :
  - Melakukan login ke usek marketing
  - Mengakses perangkat lunak aplikasi – aplikasi perkantoran
  - Memperoleh internet akses
  - Memperoleh email akses
  - Memperoleh direct line telepon
  - Mengakses dan mengupdate data pendaftaran
  - Mengakses dan mengupdate laporan serta mencetaknya.
  - Mengakses share direktori server
- Yang tidak diperbolehkan :
  - Menghapus data tanpa persetujuan pembuat data dalam share direktori
  - Memberikan data pendaftaran dan laporan baik berupa softcopy dan hardcopy pada user di luar perusahaan.
  - Memberikan hak akses terhadap softcopy dan hardcopy dokumen pada user dari luar perusahaan

**d. Instruktur (A04 – A06)**

- Yang diperbolehkan :
  - Melakukan login ke jaringan sebagai user
  - Memperoleh internet akses
  - Memperoleh email akses
  - Mengakses share direktori perusahaan
  - Mengakses materi kursus tertentu.
- Yang tidak diperbolehkan :
  - Merubah materi kursus tanpa persetujuan dan sepengetahuan General Manager

**e. Accounting(A07)**

- Yang diperbolehkan :
  - Melakukan login ke aplikasi keuangan
  - Mengakses perangkat lunak aplikasi – aplikasi akunting
  - Memperoleh internet akses
  - Memperoleh email akses
  - Mengakses share direktori server
  - Memperoleh direct line telepon
  - Menentukan penyimpanan hardcopy dokumen akunting dalam ruangan departemen akunting
  - Menentukan penyimpanan softcopy dokumen akunting dalam share direktori akunting
  - Memberikan hak akses pada hardcopy dan softcopy dokumen akunting pada user diluar departemen akunting
- Yang tidak diperbolehkan :
  - Menghapus data tanpa persetujuan pembuat data dalam share direktori
  - Memberikan hak akses terhadap softcopy dan hardcopy dokumen akunting pada user dari luar perusahaan

**f. Technical Support (A08)**

- Yang diperbolehkan :
  - Melakukan login jaringan sebagai superuser
  - Mengakses perangkat lunak aplikasi – aplikasi
  - Mengakses semua perangkat keras dalam lingkungan perusahaan
  - Memperoleh internet akses
  - Memperoleh email akses
  - Mengakses share direktori server
  - Memegang kunci ruangan server
  - Menentukan penyimpanan hardcopy dokumen teknologi informasi dalam ruangan teknologi informasi

- Menentukan penyimpanan softcopy dokumen teknologi informasi dalam share direktori
- Memberikan hak akses pada hardcopy dan softcopy dokumen teknologi informasi pada user diluar teknologi informasi
- Memberikan ijin pada staff untuk bisa mengakses internet atau jaringan dengan seijin dari technical support tersebut
- Yang tidak diperbolehkan :
  - Menghapus data tanpa persetujuan pembuat data dalam share direktori
  - Memberikan hak akses terhadap softcopy dan hardcopy dokumen perusahaan pada user dari luar perusahaan
  - Menyimpan kunci ruangan server tanpa memiliki backup kunci

**g. Training Specialist (A09)**

- Yang diperbolehkan :
  - Melakukan login jaringan sebagai user biasa
  - Mengakses perangkat lunak aplikasi – aplikasi
  - Mengakses semua perangkat keras dalam lingkungan perusahaan
  - Memperoleh internet akses
  - Memperoleh email akses
  - Mengakses share direktori server
  - Merubah isi dari materi kursus dan mengupdatenya.
- Yang tidak diperbolehkan :
  - Menghapus data materi yang belum diupdate tanpa persetujuan rapat
  - Memberikan hak akses terhadap softcopy dan hardcopy dokumen

**h. Siswa**

- Yang diperbolehkan :
  - Melakukan login jaringan sebagai user siswa (nama login berbeda tiap orang)
  - Mengakses perangkat lunak aplikasi – aplikasi tertentu sesuai dengan mata kursus yang diambil
  - Memperoleh internet akses
  - Memperoleh email akses
  - Mengakses share direktori server
- Yang tidak diperbolehkan :
  - Menginstall ataupun menguninstall program/aplikasi di komputer client.
  - Mengakses materi kursus selain dari materi kursus yang sedang di laksanakan.

## 5. Contoh SOP:

Company X

Agency-Wide

### STANDARD OPERATING PROCEDURE

NAME OF SOP: INITIAL PRODECURES IN THE EVENT OF A SUSPECTED NETWORK INTRUSION.

PURPOSE: While it is the intent of the COMPANY X's IT Department to ensure that the potential for intrusion into the COMPANY X's Wide Area Network, (WAN), and it's associated networks from the outside are minimized and that the unavailability of the data of the participating Agencies be maintained from unauthorized viewing from the inside of the WAN it is recognized that there will always be the potential for compromise. This document outlines the procedures to be carried out in the event that there is suspicion and/or evidence of such activities.

It is important to understand that compromise can come from both without and within the network. It is further important to understand that the perpetrators second task, after the initial penetration, is to hide their activity by deleting logs, preventing other access to the compromised machine, installing "back doors" to give them unfettered access to it, "sniffing" the network to catch login/password data sent in clear to help them elevate their privileges within the domain, installing "kits" that allow them to carry out other actions and even to install "rootkits" at the user or even the kernel level so that while the machine appears to be cooperating with you it is very subtly hiding the presence of the perpetrator.. In short, depending upon the skill level of the attacker, everything will be done to make the investigator(s) job more difficult or even impossible. The process documented below follows the steps it does because the more sophisticated attack systems may have self protection built into them. An example would be a backdoor listening on port 1234. It will reply to a simple SYN with a SYN/ACK, (which it is supposed to), but, if the returning ACK packet does not contain certain data in the payload, (there should be no payload on a standard ACK packet), then communication will cease, or, worse yet a clean-up routine begins where the compromised machine protects itself, (drops all packets from the network and ignores console input), while it removes all evidence of itself and then reboots to a "clean" system. While I know of no working systems such as this currently "in the wild" the potential is certainly there and as the level of sophistication rises the probability of such systems is quite high.

APPLICATION: This policy applies to all IT staff of COMPANY X and it's associated agencies.

PROCEDURES: There are occasions where a machine may give the impression that it might be compromised and there will be occasions where it is quite clear that compromise has taken place. The first act in the case of suspicion of compromise is to consult with the MIS/designated security person in the IT department to determine whether the steps this policy outlines should proceed. Prior to consultation make sure you note down exactly why your suspicions were aroused, any error messages that appeared, (the entire text), activity that was apparent etc. so that the lengthy process that follows is not gone through in vain. In short, think it through - is this really a potential compromise or is there a viable explanation for the activity, (but don't be too quick to pass it off as a "glitch", often the only indication of a compromise is a very subtle sign or signs). At this point great care must be taken to not alter the machine or carry out actions that might begin what are known as "kill processes" that clean the machine. Do the absolute minimum you can to confirm your suspicions. If you are at all unsure how to proceed at this point do nothing. Make the appropriate notes regarding how you were alerted, what you have done and call COMPANY X' MIS for advice on how to proceed.

Every step taken is to be logged. The log sheet is available from here. Logs will be created for each asset and it's components that are being investigated. Logs entries are to contain investigators initials, (legibly), date, time, action, tool, tool purpose, result, evidence location, (file name, printed document etc.). If floppy disks are used the log should indicate which floppy the evidence is located on and it's file name. Floppy Disks are to be clearly labeled EVDISKX where X is the disk number, dated and the machine name being investigated, (eg. EVDISK1 12/21/03 RM123P). CD-ROM's are to be similarly labeled. Make sure that there is no confusion caused by disk naming, (if there are 8 floppies and one CD-ROM, label them in the order of creation, Thus if the CD-ROM was the fourth disk created it should be labeled number 4). If components are removed from the computer such as the hard drive this action must be logged and a manifest created detailing date, time, action performed, signature. The drive is to be clearly labeled with the name of the machine it was removed from, the date and time of removal and the name of the person that removed it. When it is placed in or removed from storage, passed on to another person, or forensic tests are done on it the manifest must detail everything. In this way we create a chain of evidence that may be used if legal action is deemed necessary. All floppy disks should have their data backed up to a trusted and secure computer, (standalone), as soon as possible to prevent the possibility of data loss through bad floppies. When sufficient data is collected it should be written to CD-ROM to preserve it. Data written to CD-ROM for preservation purposes should be checked to ensure the write was good and labeled as "FINAL EVDISK 12/21/03 Rm123P). The original evidence disks are to be secured along with the original copy of the Incident Response Log. The Incident Response Logs should also be photocopied at the completion of each sheet. At the completion of the investigation and after the "of" sequence numbers have been assigned to the original logs the entire log for each asset is to be photocopied and secured in a location separate from the originals. The importance of these logs cannot be over-emphasized - log it, log it, log it.....

The following are the steps to be taken on each computer or server that is considered to be compromised. This document is to be printed and followed by each member of the IT response team in the order it is written unless the team leader determines that an alternative route is justified. The printed document should be shredded upon completion of the investigation.

## Initial Procedures

These procedures should be carried out prior to any investigative procedures since they make no contact with the suspect machine(s) whatsoever and rely upon totally passive methods or information that already exists.

1. The suspect machine(s) is to be left “as-is” unless, in the opinion of the MIS the damage/risk associated with such action is unacceptable. The machine therefore should remain switched on, connected to the network and no attempts are to be made to glean information from the computer locally. In short - Leave it alone until the IT Response Team leader arrives.
2. A log is to be started to document every action taken with regard to each machine and it’s components. This is especially important should the Agency consider legal action against the perpetrator(s).
3. The COMPANY X Computer Incident Response Team should be notified immediately. Team Members are detailed here.
4. The existing log files are to be secured. They are located on the workstation named XXXXXXXX in COMPANY X’s MIS’ office in the folder E:\Syslog\logs. The file is named with that days date with a .txt extension, (eg. 2003-09-10.txt). Depending upon the time of day this file can be large, (> 50Mb), so it should be copied to a remote computer. Once the copy is complete remove the network cable from the machine that the copy went to. Do not stop the logging process or disconnect the XXXXXXXX computer from the network. It needs to continue to do it’s job. XXXXXXXX’s login is XXXXXXXX with a password XXXXXXXX where X is the key combination <ALT> and the keypad numbers XXX.
5. In the subfolder of XXXXXXXX’s E:\Syslog\logs folder called Old logs you will find copies of previous days logs. On COMPANY X’ MIS’ workstation in a folder called c:\log analysis\old you will find similar copies of these files. Compare the file sizes of each file on both machines. If they are all the same, XXXXXXXX has a CD writer, cut all the files in that folder to CD, label it appropriately and secure it. If the files differ in size the compare the files of the first two copies of the logs to the final copy of the logs on COMPANYXBU in folder h:\Information system\xxxxxxx\Security Archives\firewall logs. If COMPANYXBU’s files and COMPANY X’ MIS’ files are the same size cut either to CD. If all three are different cut all three to CD for future review. Label and secure all CD’s cut.
6. At the appropriate gateway to the network Ethereal is to be started with a filter applied of “host xxx.xxx.xxx.xxx”, (without quotes), where xxx.xxx.xxx.xxx is the address of the internal machine to determine if the machine is communicating with the internet. Gateway monitors are available via computers rm258, (COMPANY X MIS’s PC), and xxxxBU,

(Backup Domain Controller in xxxxxxxx). If Ethereal indicates traffic to and from this machine Ethereal is to be left running until such time as deemed fit by the IT response team leader. The data collected is to be kept as forensic evidence.

7. If traffic is detected it may be useful to place a second version of Ethereal running on the local subnet of the target machine to determine if it is communicating with other assets inside the WAN. If it is then this data is also to be kept as forensic evidence. It may not be possible to use Ethereal on the local subnet due to the use of switches. It will be the decision of the IT response team leader whether to quickly rewire the affected machine(s) through a hub so that Ethereal can be used.

8. Secure the computer's last AIDA32 inventory file if present. This will be found on the X: drive under AidaReports. The filename will be the computer's name with a .csv extension. This details the exact hardware and much of the computer's state the last time an audit could successfully be carried out and may even contain the user name the perpetrator logged on as.

### Non-Invasive Remote data gathering Procedures

These procedures are those that are carried out from a remote workstation on the network that use tools that are active and either request information from the suspect machine(s) or glean information from it's responses to probes and scans, (or lack of responses). If possible run these tools from a workstation that can see the target machine and that all traffic can be seen by one of the Ethereal sniffers so that the packets themselves are logged for future reference. Note that the tests could be run from the appropriate Ethereal sniffer set up in the first phase though there is a small risk of packet loss. Better to use a laptop or other machine connected to the same hub as the Ethereal sniffer. Further information on the tools, their use and the command lines to execute can be found in the section "Remote Tools, their purposes, output and use".

1. NMapWin: This tool is used first in the stealth mode to glean as much information as possible about the computer without making a complete connection. If the computer has been set up with a "kill process" if unauthorized attempts to connect to it take place this should not set the process off. Note: All tools after this point elevate the risk of triggering a "kill process".

2. FScan: This will run a full connect scan to every port and grab any information it can from open ports. From here on, run the tools, log the output, check the output for items of interest and decide if this process should continue or whether the situation requires an alternative plan of action. Any alternative plan of action may only be authorized by the IT Response Team leader.

3. Cerberus Internet Scanner

4. Currentstate.vbs

5. PSInfo

6. PSList

7. PSLoggedON

8. PSLogList

## Non-Invasive Local Information Gathering Procedures.

From this point onwards it is imperative to remember that you can trust nothing on the computer(s) being investigated. Your attitude must be that every existing piece of code on the target machine has been subverted. You can't even trust the command prompt that you will use for many of the following tools. There is a trusted copy of many common applications on the CD, USE THEM.

Use floppy disks to save the data to. If no, or insufficient floppies are available, and a network connection is still operable create a share on a remote computer that you have only write access to and redirect the output there. Preferably use floppies but if using recycled floppies is required, format them on a separate, trusted computer, send the output to them and immediately copy the files to another trusted, (preferably not connected to the network), computer.

Run each tool twice. The first time redirect the output to file and examine it on a different computer. The second time run it without redirection so the output comes to the screen.

Run a quick comparison between the output to file and the output to screen to ensure they are consistent. If the output is consistent no further action is necessary. If the output is different then run the same tool three further times redirecting the output to file and number each file appropriately, (for example Netstatarm123-1.txt).

You may also notice that some of these tools may duplicate information that others provide. That is deliberate. Please do not skip steps simply because you think you have the information already..... You don't.

Finally, many of these tools are not capable of changing the state of the target computer. Others most certainly are. The goal at this stage is to glean as much information as possible about the current state and configuration of the target machine. Run the tools exactly as requested unless authorized by the IT Response Team leader. If you are uncertain whether the tool will change the system or not consult with the team leader prior to executing the tool.

Start by spawning a command prompt by selecting Start-Run and manually typing in "%path%\cmd.exe" where %path% is the location of the trusted tools. Then run the following command lines where %path% is the path to the location of the trusted tools and %path2% is the path to the output resource, (floppy, write only remote share).

NOTE: A "\*" indicates a tool that has the functionality to alter the configuration of the target. Make sure the command lines are correct prior to running the tool.

1. %path%\ipconfig /all > %path2%\ipconfigrm123.txt
2. %path%\ipxroute.exe > %path2%\ipxrouterm123.txt This will determine if IPX has been enabled.
3. (\*) %path%\arp -a > %path2%\arprm123.txt
4. %path%\hostname > %path2%\hostnamerm123.txt
5. %path%\mem /c > %path2%\memrm123.txt
6. (\*) %path%\net accounts > %path2%\netaccountsrml23.txt
7. (\*) %path%\net localgroup > %path2%\netlocalgroup.txt
8. (\*) %path%\net share > %path2%\netsharerm123.txt

9. %path%\net statistics server > %path2%\netstatsserverrm123.txt
10. %path%\net statistics workstation > %path2%\netstatsworkrm123.txt
11. (\*) %path%\net time <\\rm123> > %path2%\nettimerm123.txt (Substitute the target computer name for \\rm123 in the command line)
12. (\*) %path%\net use > %path2%\netuserm123.txt
13. (\*) %path%\net user > %path2%\netuserm123.txt
14. %path%\net view > %path2%\netviewrm123.txt
15. (\*) %path%\route print > %path2%\routeprinrm123.txt
16. %path%\fport > %path2%\fportrm123.txt
17. %path%\listdlls > %path2%\listdllsrm123.txt
18. %path%\promiscdetect > %path2%\promiscrm123.txt
19. (\*) %path%\psservice > %path2%\psservicerm123.txt
20. %path%\psgetsid > %path2%\psgetsidrm123.txt
21. dir /s > %path2%\dirXrm123.txt (do for each volume, X = volume letter including mapped drives)
22. (\*) date > %path2%\daterm123.txt
23. (\*) time > %path2%\timerm123.txt
24. vol > %path2%\volXrm123.txt (do for each volume, X = volume letter including mapped drives)
25. Tree > %path%\treeXrm123.txt (do for each volume, X = volume letter including mapped drives)

Those are the command line tools completed whose output has to be redirected to text files on trusted media. The following tools are more interactive and monitor either highly detailed activity in real time or more detailed configuration. The files can become rather large quite quickly if the activity on the machine is high so a floppy disk may be filled up quite quickly. If at all possible save these files to a remote, write only share, then cut them to CD.

1. %path%\Autoruns: This shows all the programs that are called to start during system start up. It documents the programs and the path to them.
2. %path%\filemon: This program shows file activity in real time. This file can get quite large if a lot of things are running. Run it for 5 minutes or so and save the output to the write only remote folder then cut it to CD.
3. %path%\ntpmmon: This monitors the processes and what they are doing, (opening threads, closing them etc.). If nothing is really going on then this may remain pretty much empty. It's a judgment call as to when to close it. If you are getting a lot of consistent activity from certain processes that looks "abnormal" then saving the data and closing it quite quickly may be fine and it might fit on a floppy. Remember though, it's better to have more data than less. If you aren't comfortable with the output or the amount, seek assistance.
4. %path%\procexp: This is a process explorer. It shows what processes are running and what sub-processes they have spawned. Clicking on the individual process or it's sub-processes will show all the handles or dll's the item uses. In the view menu select "Show DLL's". Create a subfolder on the remote, write only drive called Procexprm123 and then

select each process and on the file menu select “save as”. It will put the appropriate file name there for you just make sure you redirect it to the new folder on the write only share. Yes, this could be a long process but it shows all the files being used, their versions etc. and may be helpful later on.

5. %path%\regmon: This is a registry monitor. It monitors all access to the registry by all systems. It fills up quite quickly so again this may be a judgment call as to when to save the data with the rider again that too much is better than too little.

6. %path%\tdimon: This is a network interface monitor that details TCP and UDP activity at a very low level. Like other tools above it can generate a lot of log s on a busy system. Save the data away to the write only share when you feel you have enough.

This completes the formalized data gathering process from the machine(s) itself. At this point the IT Response Team Leader will make initial review of the data and decide if other or more data of certain types is required. When no other data is required the computer is to literally have the power cord pulled from the back of the machine at the power supply inlet. The computer is not to be shut down, logged off or any other way of closing it down. When computers are closed down cleanly they rewrite two entire hives of the registry and make numerous other “housekeeping” changes that are saved to the drive prior to actual shutdown. Additionally, shutdown routines could be in place to sanitize the machine in the event of a good but unexpected, (by the perpetrator), shutdown. Thus we “kill” the machine without giving it chance to alter information stored on the drive.

The final acts of this phase is to stop all the Ethereal sniffing, save the data and cut it to CD-ROM and saving all the data from any write only shares that were used to CD-ROM and removing, labeling, logging and securing the drive(s) those shares reside on.

### Drive Imaging

Once the power has been removed the hard drive(s) are to be removed from the system, labeled to indicate what they are, the act is to be logged and all the relevant details are to be noted. Two Disk images are then to be made of each disk and labeled appropriately. The act is to be logged with the appropriate details. The original drive(s) and one copy are to be secured and when, where and who secured them is to be logged. The second image can then be placed on a machine as a slave. It must not be booted to as this will change the image itself. Should the image be changed in such a way as to compromise the investigation this fact is to be logged and a new image is to be created from the stored image, (avoid using the original disk(s) ever again - that’s why we made two images in the first place). Each time a disk is moved, handed from person to person, secured or brought out of secure storage the logs are to be updated to reflect who, when, where and why the change in situation took place.

From here on it is impossible to lay down any investigative procedures since they will rely entirely upon the evidence gathered in the preceding phases. When checking the evidence you should use the “FINAL CD’s” rather than the media the evidence was originally stored

on to ensure that no changes to the evidence are inadvertently made. The original evidence media is to be logged and secured in the same fashion as the hard drive from the investigated machine.

Remote Tools, their purposes, output and use.

COMPANY X's MIS has access to all these tools. They are either on his person, on his workstation, laptop or on a CD-ROM labeled "Forensic Toolkit" in his office. COMPANY X's MIS is familiar with the use of these tools. If you are instructed to use a tool that you are unfamiliar with you are to ask for assistance prior to their use. Similarly, if you are tasked with reading the output and are unfamiliar with that you are seeing request assistance. Decisions are made throughout the process as to how to proceed that depend upon the information gained from the different systems used. If the output is misinterpreted or misrepresented an incorrect decision could be made that could render the investigation useless.

Remote, Non-Intrusive Tools

NOTE: Some of these tools require that WinPCap be installed. This is a windows packet capture driver that, at the time of writing is a version 3.2.1 and is available by searching Google for "WinPCap"

NOTE 2: Some of these remote detection tools may create alerts in the WAN's Intrusion Detection Systems.

NOTE 3: Tools with a "\*" after their name can successfully be run against machines where administrative rights are not available. In some cases the information will be complete, in other cases it will show only information that is available without administrative rights, in other circumstances all you may get is "Access Denied" Log it anyway, it's important to know what can and can't be done and may show that steps have been taken by the perpetrator to protect the computer from use by people other than himself.

1. Ethereal\*: Ethereal is a packet sniffer that is used to sniff all traffic on a network segment. It only functions effectively from a hub or a switch that can be configured to have a "bridging" port so that all traffic can be seen on the local segment. The COMPANY X WAN has two machines set aside with this capability, (rm258 and FortBU), to cover the two gateways to the network. Packets can be captured from all machines of a filter can be set to only capture traffic of certain types. These filters are based on the TCPDump syntax and can be found at <<http://home.insight.rr.com/procana/>> in the document named Designing Capture Filters for Ethereal. There is a hard copy in the black binder labeled "Security Texts" in the MIS' office. Under normal circumstances Ethereal captures packets in the background and simply shows a graph of the packets captured. In a forensic investigation it is useful to select the button to "Update the window in real time" to see the nature of the traffic involved as it occurs. When saving the data save it in the default

TCPDump format which allows the data be be reloaded into many other analysis tools and even to rerun the entire session if necessary.

2. NMapWin\*: NMapWin is the WIN32 port of the venerable NMap by Fyodor. It is the most powerful scanner/OS detection system currently available. For forensic purposes the following settings are advised. Select a SYN Stealth Scan from the Scan tab, “Don’t ping” from the discover tab, “OS Detection” and “Very Verbose” from the Options tab and select Output file and name it as a:\NMaprm123p.txt. Put the IP Address of the target in the Host line and begin the scan.

3. FScan\*: FScan is a command line port scanner that has some interesting features. From it’s home directory type “fscan -?” for a list of all it’s parameters. A recommended command line would be `fscan -bp 1-65535 -u 1-65535 -o a:\fscanrm123p.txt -s rm123`. This would scan all TCP and UDP ports from 1 through to 65535 and grab the available banners of any open ports, show any RST’s returned from the target, (a lack of which may imply there is a “firewall” in place), and write all the results to a file called fscanrm123p.txt on the floppy disk.

4. Cerberus Internet Scanner\*: This tool looks at services commonly available and extracts as much information as is available with or without administrative rights. With administrative right a lot can be determined about the general “look” of the target and some useful information comes with only guest rights. The report is written to the home folder’s “Reports” folder and is named using the IP address of the target with an HTML extension. The report file should be moved to an evidence floppy.

5. Currentstate.vbs: This is a script the MIS wrote himself to automatically extract information remotely and in a non-intrusive manner from a computer you have administrative rights over. Run it from it’s home directory using the command line “`cscript currentstate.vbs`” and you will be prompted for the IP address of the target machine, the full name of the output file, your full name, the administrators login name and the administrators password. This pulls a lot of relevant information regarding the current state of a remote machine right down to which processes belong to which threads and could be very useful in a forensic investigation.

6. PSInfo: PSInfo gives some additional information regarding the makeup of a machine that others above may not. Rights are required to the target machine. Recommended command line is “`psinfo \\rm123p > a:\PSInform123p.txt`”. Note that the results have to be piped to the output file.

7. PSList: PSlist dumps the running processes, their PID’s, kernel time, user time, idle time etc. Recommended command line is “`pslist \\rm123p > a:\SPListrm123p.txt`”. It requires rights to the target machine.

8. PSLoggedon\*: PSloggedOn can reveal information about locally and remotely logged on users without administrative privileges on the target machine. Recommended command line is “`psloggedon \\rm123p > a:\psloggedonrm123p.txt`”

9. PSLogList: PSlogList can retrieve the entire existing event logs of a remote computer with administrative rights, (it may also be able to with limited rights). Recommended command line is “`psloglist \\rm123p > a:\psloglist.txt`”

## BIBLIOGRAPHY

### Book

- [RON05] Ronald L. Krutz, Russell Dean Vines. **The CISSP® Prep Guide: Gold Edition**. Wiley Publishing, Inc. 2003.

### Sites:

1. **Building Secure ASP.NET Applications: Authentication, Authorization, and Secure Communication** <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/SecNetch02.asp> Last Visited 11 November 2005
2. **[OSMOSE]: Security framework- Architecture & APIs (Model) document** <http://mail-archive.objectweb.org/architecture/2004-04/msg00004.html> Last Visited 11 November 2005
3. **Security Models and Architecture** [www.cccure.org/Documents/Hal\\_Tipton/Intro2.pdf](http://www.cccure.org/Documents/Hal_Tipton/Intro2.pdf) Last Visited 11 November 2005
4. **AttackPrevention: Security Architecture and Models** [http://www.attackprevention.com/article/Security\\_Architecture\\_and\\_Models-160.html](http://www.attackprevention.com/article/Security_Architecture_and_Models-160.html)
5. **Network Security- A Guide for Small and Mid-sized Businesses** Jim Hietala <http://www.sans.org/rr/whitepapers/basics/1539.php> Last Visited 11 November 2005
6. Example Forensic SOP/Procedur. AntiOnline. <http://www.antionline.com/forumdisplay.php?s=0582c3f9637bdc413320af3cbeb9617a&forumid=59> Last Visited 22 December 2005.