**MANAJEMEN SUMBER DAYA INFORMASI**

 **( Materi Perkuliahan Sesi 2)**

**Definisi**

 IRM (Information Resources Management) merupakan metodologi siklus hidup yang digunakan untuk menciptakan system yang menghasilkan informasi yang berkualitas. IRM adalah konsep manajemen sumber informasi yang mengenal informasi sebagai sumber organisasional utama yang harus dikelola dengan tingkat kepentingan yang sama seperti sumber organisasional dominan lain seperti orang, keuangan, peralatan dan manajemen.[[1]](#footnote-2) Sumber daya informasi terdiri atas :

* Perangkat keras dan perangkat lunak komputer
* Spesialis informasi

Istilah spesialis informasi digunakan untuk menggambarkan pegawai perusahaan yang sepenuh waktu bertanggung jawab mengembangkan dan memelihara sistem berbasis komputer, yg terdiri dari :

1. Analis Sistem
2. Pengelola Database
3. Spesialis Jaringan
4. Pemakai
5. Programmer
6. Operator
7. Komputer
* Pemakai

Pemakai terdiri dari pemakai awam (end user)  dan administrator sistem. End User Computing (UEC)  adalah pengembangan seluruh atau sebagian sistem berbasis komputer oleh pemakai (user). EUC berkembang karena beberapa alasan yaitu meningkatnya pengetahuan tentang computer, antrian jasa informasi, perangkat keras yang murah, perangkat lunak.

* Fasilitas

Fasilitas adalah prasarana atau wahana untuk melakukan atau mempermudah sesuatu. Fasilitas bisa pula dianggap sebagai suatu alat. fasilitas biasanya dihubungkan dalam pemenuhan suatu prasarana umum yang terdapat dalam suatu perusahaan-perusahaan ataupun organisasi tertentu.

* Database

Sekumpulan data yang terintegrasi yang diorganisasi untuk memenuhi kebutuhan pemakai untuk keperluan organisasi

* Informasi

Jaringan computer dan komunikasi data, Informasi, Seiring dengan berkembangnya teknologi komputer yang memiliki kemampuan proses yang lebih cepat, maka muncul konsep SIM yang menyadari bahwa aplikasi komputer harus diterapkan untuk tujuan utama menghasilkan informasi manajemen disetiap area fungsional dan level aktivitasnya.

## Konsep manajemen sumber daya informasi

Manajemen sumber daya informasi (information resource management) atau IRM adalah aktivitas yang dijalankan oleh manajer pada semua tingkatan dalam perusahaan dengan tujuan mengidentifikasi, memperoleh, dan mengelola sumber daya informasi yang diperlukan untuk memenuhi kebutuhan pemakai.

 Agar perusahaan dapat sepenuhnya mencapai IRM, perlu ada serangkaian kondisi tertentu, yakni:

* Kesadaran bahwa keunggulan kompetitif dapat dicapai melalui sumber daya informasi yang unggul.
* Kesadaran bahwa jasa informasi adalah suatu bidang fungsional utama.
* Kesadaran bahwa CIO adalah eksekutif puncak.
* Strategi untuk mendorong dan mengelola end user computing.

Usaha-usaha yang diperlukan untuk mencapai IRM yang sukses adalah :

* Perusahaan berusaha untuk menggunakan informasi untuk mencapai keuntungan kompetitif.
* Para eksekutif harus menyadari bahwa pelayanan informasi sebagai area fungsional.
* Para eksekutif harus mengakui keberadaan CIO.
* Para eksekutif harus memasukkan sumber-sumber informasi dalam perencanaan strategi.
* Adanya perencanaan strategi formal untuk sumber-sumber informasi.
* Perencanaan strategi juga untuk mengatur pemakai komputer.

IRM akan berhubungan dan bekerja sama dengan :

1. Lingkungan perusahaan
2. Eksekutif perusahaan
3. Area Bisnis
4. Sumber daya informasi
5. Pemakai

Aktifitas IRM dihubungkan dengan 2 hal, mencakup :

1. Information services department (ISD)
2. End-user departement, unit dan tim

**Information services department (ISD)**

 ISD merupakan organisasi jasa yang mengelola infrastruktur IT yang diperlukan untuk mengarahkan aplikasi IT bagi end-user. Dengan demikian, hubungan antara ISD dan end-user merupakan suatu keharusan, hal ini dikemukakan oleh Wysocki De Michiell (1996). Hal ini bukan merupakan tugas yang mudah karena ISD pada dasarnya suatu organisasi secara teknis mungkin tidak memahami bisnis tersebut dan usernya. Disisi lain, user mungkin tidak memahami teknologi informasi.

 Untuk mendorong hubungan antara ISD dan end-user, organisasi dapat menerapkan beberapa strategi, antara lain:

1. Memperkenalkan end-user adanya unit yang mendukung koordinasi kualitas asuransi, administrasi data dan sistem kantor.
2. Memperkenalkan end-user adanya unit training dan pengembangan yang mengarahkan pada training dan penghargaan dalam software IS.
3. Memberikan prioritas dan visibilitas yang tinggi bagi end-user.
4. Training para pekerja ISD untuk memahami bisnis.
5. Mengimplementasikan tim khusus yang menangani konflik yang secara cepat menangani konflik ISD/ End-user.
6. Mendorong CIO sebagai anggota dari tim organisasi eksekutif.
7. Mendorong para pekerja ISD untuk mengambil keputusan meskipun memiliki referensi yang minim.
8. Mengembangkan perencanaan perbaikan bagi masing-masing end-user untuk meminimumkan resiko pada saat sistem gagal.

 Untuk mencapai misi dalam ekonomi digital, ISD perlu untuk berubah. Rockart et al (1996) memberikan 8 hal yang harus dilakukan dalam hal ISD pada era digital yang mengarahkan pada new IT organization:

1. Mencapai kesetaraan strategic 2 arah

Kesetaraan strategic mencakup 2 hal yaitu kesetaraan antara strategi IT dengan strategi bisnis yang dilakukan organisasi. Dua hal ini harus dicapai oleh eksekutif dalam organisasi yang berbasis IT.

1. Mengembangkan hubungan yang efektif den gan manajemen lini.

Personil yang terlibat dalam IT harus mengembangkan hubungan yang kuat dengan end-user. Tujuannya untuk mencapai kapabilitas dalam bisnis dan teknologi yang diintegrasikan guna mencapai solusi yang efektif dalam memecahkan masalah-masalah organisasi.

1. Pengembangan dan implementasi sistem baru secara cepat.

Aplikasi inovatif harus dikembangk an dengan cepat dan efektif melalui ISD, bagi user dan outsourcers. Sistem yang dihasilkan mencakup pengembangan sistem secara efektif, procurement, dan integrasi.

1. Membangun dan mengelola infrastruktur.

ISD bertanggungjawab untuk menciptakan dan mengelola infrastruktur yang efektif. Infrastruktur yang memadai akan mendukung pekerjaan yang dilakukan dalam suatu network/ jaringan. Untuk mencapai hal ini organisasi menghasilkan posisi baru yaitu Chief Network Officer (CNO) yang hasilnya kemudian dilaporkan pada CIO.

1. Meningkatkan keterampilan kembali bagi orgaisasi yang bergerak di bidang IT.

Peranan baru dalam ISD memerlukan k eter ampilan baru. Memberikan training berulang merupakan solusi guna menemukan karyawan dengan keterampilan teknologi baru yang merupakan tugas yang sulit.

1. Mengelola hubungan dengan vendor.

Karena outsourcing merupakan pilihan yang banyak diterapkan, khususnya untuk aktivitas ISD yang tidak memiliki cuup waktu dan keahlian sehingga perlu adanya hubungan dengan vendor yang tidak sekedar hanya transaksional dan kontraktual tetapi mengarah pada k egiatan strategic.

1. Meningkatkan kinerja yang tinggi.

ISD seharusnya menggunakan metode manajemen modern untuk memperbaki dengan kegiatan operasi. Sistem harus dikembangkan dengan cepat dan dengan cara yang paling efisien.

1. Mendesain dan mengelola kembali organisasi IT.

**End-user departement, unit dan tim**

Tingkat-tingkat Kemampuan Pemakai Akhir, digolongkan 4 yaitu :

* Pemakai akhir tingkat menu (*menu-level end user*)

Tidak mampu menciptakan perangkat lunak sendiri, tetapi dapat berkomunikasi dengan perangkat lunak jadi dengan menggunakan menu-menu seperti yang ditampilkan oleh perangkat lunakberbasis Windos dan Mac

* Pemakai akhir tingkat perintah (*command level end user*)

Dapat menggunakan bahasa perintah untuk melaksanakan operasi aritmetika dan logika pada data.

* Pemakai akhir tingkat Programer (*end user programmer*)

Dapat menggunakan bahasa pemrograman seperti C++ dan mampu mengembangkan program-program yang disesuaikan dengan kebutuhan mereka sendiri.

* Personil pendukung fungsional (*fungsional support personnel)*

Merupakan spesialis informasi, tetapi mereka berdedikasi pada area pemakai tertentu dan melapor pada manajer fungsional mereka.

EUC memberi manfaat bagi perusahaan dalam dua cara utama:

1. Menyeimbangkan Kemampuan dan Tantangan

Pemindahan beban kerja dari pengembangan system ke area pemakai membebaskan para spesialis untuk berkonsentrasi pada system yang rumit dan berlingkup organisasi, sehingga mereka dapat bekerja lebih baik pada area bidang tersebut. Para spesialis informasi juga dapat mencurahkan lebih banyak waktu untuk memelihara system yang ada.

1. Mengurangi Kesenjangan Komunikasi

Kesulitan komunikasi antara pemakai dan para spesialis informasi telah mengganggu pengembangan system sejak masa awal adanya komputer. Pemakai memahami bidang permasalahan dengan lebih baik, sebaliknya, spesialis adalah pakar teknologi tetapi tidak menguasai bidang permasalahan. Dengan membiarkan pemakai mengembangkan aplikasi mereka sendiri, tidak ada kesenjangan komunikasi karena tidak diperlukan komunikasi.

 Ketika para pemakai menegmbangkan system mereka sendiri, perusahaan dihadapkan pada sejumlah resiko, yakni:

* + - 1. Sistem yang buruk sasarannya
			2. System yang buruk rancangan dan dokumentasinya
			3. Penggunaan Sumber daya Informasi yang tidak efisien
			4. Hilangnya integritas data
			5. Hilangnya keamanan
			6. Hilangnya pengendalian

Sebagian besar aplikasi end-user terbatas pada:

* Sistem pendukung keputusan (DSS) yang relatif mudah
* Aplikasi virtual office yang memenuhi kebutuhan perseorangan.

 Selebihnya adalah tanggung jawab spesialis informasi untuk bekerja sama dengan pemakai dalam mengembangkan:

* Aplikasi SIM dan SIA
* DSS yang rumit
* Virtual office yang memenuhi kebutuhan organisasi
* Sistem berbasis pengetahuan



Gambar 1. Konsep IRM

**Mengelola sumber daya informasi**

 Unit yang mengelola sumber daya informasi disebut jasa informasi, dikelola oleh manajer. Praktek yang umum terjadi sekarang adalah membentuk jasa informasi sebagai suatu bidang fungsional utama dan menyertakan manajer puncaknya dalam kelompok eksekutif, yang membuat keputusan-keputusan penting perusahaan.

Istilah chief information officer (CIO) merupakan salah satu eksekutif tingkat puncak perusahaan, bertanggung jawab atas salah satu area fungsional utama jasa informasi. CIO merupakan anggota komite eksekutif dan bekerjasama dengan para eksekutif lain dalam perencanaan strategis. Rencana bisnis strategis menyatukan informasi sebagai sumberdaya yang perlu digunakan untuk mendapatkan keunggulan kompetitif, dan didukung oleh suatu rencana strategis untuk sumberdaya informasi. Adapun tugas dari CIO antara lain :

* + Mempelajari bisnis dan teknologinya
	+ Menjalin kemitraan dengan unit bisnis dan manajemen
	+ Fokus memperbaiki proses bisnis dasar
	+ Memperkirakan biaya system informasi dalam bisnis
* Membangun kredibilitas dengan mengirim service yang terpercaya.

Programmer

Analis

Sistem

Manajer PemeliharaanSistem

Manajer Operasi Komputer

Personil

Operasi

Manajer Jaringan

Spesialis

Jaringan

Manajer Administrasi Database

Pengelola

Database

Programmer

Analis

Sistem

Manajer

Pengembang

Sistem

**C . I . O**

Gambar 2. Struktur Organisasi Fungsional Jasa Informasi

 Spesialis informasi merupakan istilah untuk menggambarkan pegawai perusahaan yang bertanggung jawab mengembangkan dan memelihara system berbasis komputer. Ada 5 golongan utama spesialis informasi:

* Analis system (system analist)

Analis system adalah pakar dalam mendefinisikan masalah dan menyiapkan dokumentasi tertulis mengenai cara komputer membantu pemecahan masalah. Analis system bekerja sama dengan pemakai mengembangkan system baru dan memperbaiki system yang ada sekarang.

* Pengelola database (database administrator)

Pengelola database mempunyai tugas untuk memelihara database dan bekerja sama dengan pemakai dan analis system menciptakan database yang berisi data yang diperlukan untuk menghasilkan informasi bagi pemakai. Database merupakan suatu kumpulan data komputer yang terintegrasi, diatur dan disimpan menurut cara yang memudahkan pengambilan kembali.

* Spesialis jaringan (Network specialist)

Spesialis jaringan bekerja sama dengan analis system dan pemakai membentuk jaringan komunikasi data yang menyatukan berbagai sumber daya komputer yang tersebar.

* Programmer

Menggunakan dokumentasi yang disiapkan oleh analis system untuk membuat program

* Operator

Mengoperasikan peralatan komputer berskala besar seperti komputer mainframe. Operator memantau layar komputer, mengganti ukuran kertas di printer, mengelola tape dan disk storage, dll.

 CIO dapat menghadapi tantangan langsung dan menyediakan dukungan informasi berkualitas dengan mengikuti suatu strategi yang terdiri dari elemen-elemen :

1. Menekankan manajemen kualitas dari sumber daya informasi dengan mengidentifikasi kualitas kebutuhan dari pelanggan informasi eksternal dan internal.
2. Mencapai ikatan pemakai yang kuat dengan memastikan bahwa tujuan IS sesuai dengan tujuan pemakai dan memastikan bahwa aplikasi bernilai strategis bagi perusahaan mendapatkan dukungan kualitas tertinggi serta menekankan pengembangan aplikasi bersama.
3. Memperkuat ikatan eksekutif dengan menjadi pakar dalam bisnis perusahaan dan menyediakan dukungan informasi perusahaan bagi eksekutif perusahaan.
4. Menyusun tim IS yang memiliki kemampuan teknis dan manajerial yang diperlukan untuk mengintegrasikan sumber daya informasi.
5. Menyusun staf IS yang kompeten dalam teknologi dan metodologi yang canggih untuk menyediakan dukungan user.
6. Membangun sistem informasi pelayanan informasi yang memungkinkan CIO dan manajemen IS mengelola sumber daya informasi dalam lingkungan perusahaan.

**Model Sistem Sumber Daya Informasi**

 Sistem yang menyediakan informasi mengenai sumber daya informasi perusahaan kepada para pemakai diseluruh perusahaan.

Sistem

Informasi

Akuntansi

Subsistem

Riset

Sumber Daya

Informasi

Subsistem

Intelijen

Sumber daya

Informasi

Sumber

Internal

Sumber

Lingkungan

Subsistem Input

**D**

**A**

**T**

**A**

**B**

**A**

**S**

**E**

Subsistem

Perangkat

Lunak

Subsistem

Sumber Daya

Manusia

Subsistem

Data dan

Informasi

Subsistem

Sumber Daya

Terintegrasi

Subsistem

Perangkat

Keras

## U S E R

**Subsistem**

**Output**

Gambar 3. Model sistem IRM

Keterangan :

*Subsistem Input :*

1. Sistem Informasi Akuntansi yaitu mengumpulkan data internal yang menjelaskan unit jasa informasi dan data lingkungan yang menjelaskan transaksi unit tersebut dengan para pemasoknya.
2. Subsistem Riset Sumber Daya Informasi menjelaskan kegiatan yang terdiri dari proyek-proyek riset didalam perusahaan yang selanjutnya menentukan kebutuhan user dan kepuasan user.
3. Subsistem Intelijen Sumber Daya Informasi menjelaskan fungsi yang berhubungan dengan pengumpulan informasi dan elemen-elemen di lingkungan perusahaan khususnya elemen-elemen yang berinteraksi dengan jasa informasi.

Elemen-elemen ini meliputi :

* + Pemerintah.
	+ Pemasok.
	+ Serikat Pekerja.
	+ Masyarakat Global.
	+ Pelanggan.
	+ Pesaing.
	+ Masyarakat Keuangan.
	+ Pemegang Saham.

*Subsistem Output :*

* + 1. Subsistem Perangkat Keras menyiapkan output informasi yang menjelaskan sumber daya perangkat keras. Perangkat Lunak yang digunakan dalam subsistem ini dapat berupa query language, pembuatan laporan dan model matematika.
		2. Subsistem Perangkat Lunak menyiapkan output informasi yang menjelaskan sumber daya perangkat lunak. Output informasi terutama berbentuk jawaban atas database query dan laporan periodik.
		3. Subsistem Sumber Daya Manusia menyediakan informasi tentang para spesialis informasi perusahaan.
		4. Subsistem Data dan Informasi menyiapkan output yang menjelaskan sumber daya data dan informasi yang berada di database pusat.
		5. Subsistem Sumber Daya Terintegrasi menyatukan informasi yang menjelaskan sumber daya hardware, software, SDM serta data dan informasi.

**Perencanaan Strategis Sumber Daya Informasi**

SPIR (Strategic Planning for Information Resourcers)

* Perencanaan strategi merupakan perencanaan yang paling memerlukan perhatian. Karena memerlukan perkiraan yang matang untuk dapat mencapai tujuan organisasi pada masa sekarang dan akan datang.
* Saat menerapkan SPIR, rencana strategis untuk jasa informasi dan rencana strategis untuk perusahaan dikembangkan bersamaan.
* Perencanaan strategis disebut juga perencanaan jangka panjang karena mengidentifikasikan tujuan-tujuan yang akan memberikan perusahaan posisi yang paling menguntungkan dlm lingkungannya serta menentukan strategi-strategi untuk mencapai tujuan-tujuan tersebut.
* Gagasan utama dari SPIR adalah adanya hubungan antara tujuan perusahaan secara keseluruhan dengan sumber-sumber informasi. Sumber-sumber informasi harus digunakan untuk mencapai tujuan.
* Pendekatan-pendekatan Top down :
	+ BSP IBM (Business Systems Planning)

Setiap manajer diinterview untuk menentukan kebutuhan informasi, kemudian system diimplementasikan sesuai dengan kebutuhan informasi.

* + CSF (Critical Success Factor)

Perencanaan sumber informasi dengan mengidentifikasi kunci keberhasilan dan kegagalan.

* + Transformasi susunan strategis
	+ SLC (Siclus Life Circle) yang diperluas

Gambar 4. Perencanaan Strategis Sumber daya Informasi

**KEAMANAN SUMBER DAYA INFORMASI**

**Mengamankan Sumberdaya Informasi**

 Tujuan-tujuan keamanan sistem *(systems security)* mengacu pada perlindungan terhadap semua sumberdaya informasi perusahaan dari ancaman oleh pihak-pihak yang tidak berwenang. Tujuan-tujuan keamanan yaitu :

* Kerahasiaan

Perusahaan berusaha melindungi data dan informasi dari orang-orang yang tidak berhak.

* Ketersediaan

Menyediakan data dan informasi bagi mereka yang berwenang untuk menggunakannya.

* Integritas

semua subsistem harus menyediakan gambaran akurat dari sistem fisik yang diwakilinya.

Ancaman keamanan :

* pengungkapan tidak sah dan pencurian
* penggunaan tidak sah
* penghancuran tidak sah dan penolakan jasa
* modifikasi jasa.

Jenis modifikasi yang sangat mencemaskan disebabkan oleh perangkat lunak yang merusak *(malicious software).* Perangkat lunak yang merusak terdiri dari program lengkap atau segmen kode yang melaksanakan fungsi yang tidak dikehendaki pemilik sistem. Beberapa perangkat lunak perusak adalah virus antara lain : *tradoars, logic bombs, Trojan horses, worms, bacteria,* dan *rabbits.*

Pengendalian akses dicapai melalui suatu proses tiga langkah yang mencakup :

* identifikasi pemakai
* pembuktian keaslian pemakai
* otorisasi pemakai.



Gambar 5. Proses Pengendalian Hak Akses

Nama ancaman tingkat tinggi *(high-grade threats)* diberikan kepada para penjahat komputer, karena :

* mereka memiliki sumberdaya uang, personalia, dan teknologi tersembunyi *(clandestine)* yang ekstensif
* mereka lebih tertarik pada keuntungan jangka panjang daripada hasil segera
* mereka sangat mahir menghindari pengamanan fisik dan prosedural.

 Di dalam penggunaan komputer sering ada pelanggaran. Database pribadi tidak selalu digunakan secara hati-hati. Untuk mempraktekkan etika komputer, CIO itu :

1. Memformulasikan kode prilaku yang menentukan kewajiban etika IS.
2. Menetapkan aturan prosedur yang berhubungan dengan praktek praktek yang telah dikritik dari sudut etika, seperti penggunaan jasa komputer pribadi dan hak milik program dan data komputer.
3. Mengidentifikasi hukuman, seperti teguran, penghentian, dan tuntutan hukum pelanggaran aturan etika.
4. Menetapkan sistem penghargaan untuk prilaku etika yang baik.
5. Membuat program-program etika seperti pelatihan dan bacaan wajib yang menekankan etika serta memungkinkan spesialis informasi untuk memenuhi harapan tersebut.
6. Membuat program pendidikan kejahatan komputer yang menginformasikan para pegawai mengenai peraturan hukum yang mempengaruhi operasi komputer.
7. Memasang suatu sistem yang menetapkan pertanggung jawaban *(accountability)* tiap spesialis informasi atas tindakannya.
8. Mendorong program rehabilitasi bagi para pelanggan etika.
9. Mendorong partisipasi dalam menghimpun profesional.
10. Menjadi teladan.

Tindak kejahatan dan kriminalitas dalam computer ada 4 tipe:

1. Komputer dapat menjadi target kriminalitas

Contoh: computer dapat dicuri, dirusak atau virus yang dapat merusak data.

1. Komputer dapat menjadi medium dari tindakan perusakan dengan menciptakan lingkungan yang memungkinkan tindak criminal terjadi.

Contoh: kesalahan data yang dimasukkan dalam sistem computer mengarah pada kesalahan atau kek eliruan dalam menguji kondisi keuangan dalam perusahaan.

1. Komputer dapat menjadi alat (tool) yan g memperlancar tindak criminal.

Contoh: Komputer yan g digunak an dalam merencanakan kejahatan, tetapi kriminalitas tidak melibatkan computer.

1. Komputer dapat digunakan untuk intimidasi.

Contoh: stockholder mencuri $50 juta dari kliennya karena memiliki program computer yang dapat meningkatkan ROI (Return on Investment) 60% setiap bulan.

Hacker Vs. Cracker

Kejahatan dalam computer dapat ditunjukkan melalui:

* Outsider yang melakukan penetrasi dalam sistem computer (seringkali melalui jaringan computer)
* Insider yang memperkenalkan penggunaan sistem computer tetapi dengan cara memperkenalkan cara penggunaan yang salah

 Proteksi Sistem Informasi Perlu strategi perlawanan bagaimana usaha untuk melindungi sistem informasi melalui:

1. *Prevention and deterrence*
2. *Detection*
3. *Limitation*
4. *Recovery*
5. *Correction*

**Implementasi Security**

 Audit merupakan bagian penting dari control sistem. Dalam setting organisasi biasanya menunjukkan pengujian dan pengecekan secara periodic dari kegiatan akuntansi dan keuangan khususnya pada kegiatan auditing.

* Internal auditor: biasanya karyawan perusahaan yang merupakan anggota ISD.
* Eksternal auditor: orang luar dari perusahaan

**CONTOH KASUS**

 Implementasi IRM pada perbankan khususnya bank BCA sebagai bank transaksional yang menawarkan rangkaian jasa yang luas untuk memenuhi kebutuhan-kebutuhan spesifik para nasabahnya. Sebagai lembaga intermediari keuangan, BCA telah bekerja keras untuk memperkuat sisi kredit dengan mempersiapkan berbagai paket yang menarik bagi nasabah yang potensial. Bank tersebut memiliki sejumlah keunggulan yang menjadi kunci keberhasilannya dalam menyediakan jasa-jasa yang berguna, efisien dan mudah.

Sumber daya informasi yang ada pada bank bca antara lain :

* Perangkat keras

Komputerisasi yang ada di dalam jaringan yang luas dari kantor cabang dan kantor cabang pembantu di seluruh Indonesia, serta memiliki sekitar 6.710 ATM tunai maupun non-tunai serta ATM Setoran Tunai yang disediakan di berbagai lokasi strategis di seluruh Indonesia.

* Perangkat lunak komputer

 Software yang ada pada bank bca antara lain :

1. Aplikasi intenet banking
2. Mobile banking
3. Sistem core banking mulai dibangun dengan menggunakan software Marshal & Illsley Bank dari Amerika Serikat. Dengan begitu, bagian back office BCA sudah bisa terintegrasi. Misalnya, sistem produk (tabungan) Tahapan atau giro sudah terintegrasi ke pembukuannya (modul general ledger/GL). Karena itu, begitu terjadi transaksi, tidak harus di-posting lagi ke modul GL, karena sistem akan melakukannya secara otomatis.
* Spesialis informasi

Tim TI BCA pun dibentuk dan dibagi dalam tiga kelompok, yang saling terintegrasi meski fungsi kerjanya berbeda-beda yaitu:

1. Grup Aplikasi, yang fungsi utamanya membangun atau membuat program aplikasi (software). Misalnya, untuk produk Tahapan, Grup Aplikasi inilah yang merancangnya. Mulai dari pembuatan program untuk nomor rekening, inquiry saldo, perhitungan undian, bunga, biaya administrasi, hingga program pencetakan pada buku tabungan. Boleh dibilang Grup Aplikasi ini merupakan kelompok besar karena diperkuat sekitar 100 orang staf. Mengingat begitu banyaknya jenis aplikasi, maka grup ini dibagi lagi menjadi tiga subgrup antara lain :
* Subgrup Aplikasi Pertama lebih fokus menggarap aplikasi untuk produk pendanaan, seperti Tahapan, Tapres, giro dan deposito.
* Subgrup Aplikasi Kedua berkonsentrasi mengembangkan aplikasi kredit, mulai dari kredit ritel, korporat, atau kartu kredit.
* Subgrup Aplikasi Ketiga bertugas khusus menyiapkan aplikasi sesuai dengan kebutuhan internal BCA seperti aplikasi inventori dan SDM.
1. Grup Sistem, Network dan Operasional (SNO). Grup ini terdiri dari sekitar 60 orang. Grup SNO inilah yang menentukan hal-hal seperti back-end-nya akan menggunakan mesin apa, middleware-nya pakai sistem apa, hardware yang dipilih apa, dan sebagainya. Adapun staf network punya tugas pokok mengelola sistem jaringan. Termasuk, misalnya, menentukan jenis jaringan yang cocok untuk suatu kantor cabang. Biasanya, penentuan jenis jaringan ini tergantung pada volume transaksi dan besar aset kantor cabang. Untuk sistem jaringan cabang-cabang yang besar umumnya menggunakan fiber optik, jaringan multiprotocol label switching (MPLS), dan wireless wide area network (WAN). Menurut Hermawan, sebenarnya penggunaan sistem jaringan yang berbeda-beda itu baru dilakukan dalam 2-3 tahun terakhir. Ini sejalan dengan perkembangan BCA, dari segi jumlah nasabah, transaksi cabang, dan sebagainya. Adapun jaringan VSAT sendiri masih tetap digunakan sebagai back up. Untuk jaringan serat optik, BCA menggunakan fasilitas milik Indosat; serta jaringan MPLS dari Telkom dan icon+ (anak usaha PLN).
2. Grup Sekuriti, Grup beranggota 20 orang inilah yang menentukan: siapa yang berhak mengakses, bagaimana kebijakan password dan antivirus; bagaimana agar sistem tidak dikerjai orang (di-hack) dan sebagainya.
* Pemakai

Pemakai terdiri dari pemakai awam (end user) dan administrator sistem. End-User pada bank bca terdiri dari karyawanan (operator) dan nasabah. Sedankan administrator sistem merupakan staff IT yang ada pada bank bca tersebut. Tugas dari administrator sistem antara lain :

1. Merancang dan melakukan instalasi hardware dan software
2. Mendefinisikan dan megidentifikasikan atribut yang digunakan oleh user
3. Melakukan dokumentasi konfigurasi sistem
4. Menjaga tingkat keamanan instalasi komputer
5. Melakukan tuning kinerja sistem komputer
6. Meyakinkan infrastruktur dan jaringan komputer dalam keadaan baik
7. Melakukan backup dan restore
8. Menjawab masalah teknis dan memecahkan masalah
9. Melakukan audit software dan hardware
10. Mengidentifikasi ancaman dan tanggap terhadap isu yang berhubungan dengan system
* Fasilitas

 Fasilitas yang ada pada bank bca antara lain :

1. Simpanan

Rekening TAHAPAN, Rekening TAPRES, Rekening Giro,Deposito Berjangka dan Sertifikat Deposito.

1. Kartu Kredit

BCA Card, BCA Master Card, BCA Visa, BCA JCB

1. Perbankan Elektronik

ATM BCA, Debit BCA, Tunai BCA, klikBCA Internet banking, m-BCA mobile banking, BCA Link, Call Center

1. Layanan Transaksi Perbankan

Safe Deposit Box (SDB), Pengiriman Uang, Travelers Cheques, Inkaso dan Kliring, mata uang asing.

1. Fasilitas Kredit

KPR, KKB, Kredit Modal Kerja, Kredit Sindikasi, Kredit Ekspor, Trust Receipt, Kredit Investasi.

1. Bank Garansi

Bid bond, Payment Bond, Advance Payment Bond, Performance Bond, dan Pusat Pengelolaan Pembebasan dan Pengembalian Bea Masuk (P4BM).

1. Fasilitas Ekspor-Impor

LC, Negosiasi, Bill Discounting, Documentary Collections, Bankers Acceptance.

1. Fasilitas Valuta Asing

Spot, Forward, Swap, dan produk derivative lain

* Database

Database yang ada pada bank bca terdiri dari :

1. Data keuangan, seperti data transaksi perbankan,
2. Data SDM, seperti data karyawan dan nasabah
3. Data perusahaan, seperti data inventaris dan lain-lain
* Informasi

BCA selalu mempertimbangkan kebutuhan nasabah yang selalu berubah. Lebih jauh lagi, bank tersebut terus menyempurnakan setiap produk atau jasanya dengan menambahkan berbagai fitur baru untuk meningkatkan kenyamanan nasabah dalam menggunakannya, seperti semakin banyak fasilitas yang sediakan di ATM, KlikBCA Individual Internet banking, m-BCA mobile banking, dan sebagainya.

Peran CIO pada bank bca antara lain :

* mampu mentransformasikan aplikasi, layanan, dan infrastruktur teknologi informasi (TI) agar menjadi fleksibel, dapat diperluas, dan aman.
* harus siap mendukung model bisnis perusahaan yang berubah-ubah (disruptif), termasuk akuisisi, merger, dan divestasi.

Keamanan sistem informasi

1. Sistem Pengamanan

BCA menggunakan 3 (tiga) lapis sistem pengamanan untuk melindungi akses dan transaksi Anda di internet banking BCA yaitu :

* Secure Socket Layer (“SSL”) SSL adalah teknologi pengamanan yang ‘mengacak’ jalur komunikasi antar komputer sehingga tidak dapat dibaca oleh pihak lain.
* User ID dan Personal Identification Number (“PIN”)
* One Time Password yang dihasilkan oleh KeyBCA One-time Password adalah teknologi pengamanan yang selalu menghasilkan password yang berbeda setiap kali alat/token pengamannya digunakan.

Karena banyaknya variasi browser internet yang ada, sulit untuk menyediakan internet banking yang mengikuti keamanan masing-masing browser. Saat ini BCA hanya menyediakan sarana internet banking yang lebih cocok diakses dengan menggunakan Microsoft Internet Explorer versi 6 atau yang terbaru. BCA mohon maaf atas ketidaknyamanan ini.

2. Proteksi Komunikasi Internet Banking BCA

BCA menggunakan teknologi enkripsi Secure Socket Layer (SSL) 128 bit untuk memproteksi komunikasi antara komputer Anda dan server BCA selama Anda mengakses internet banking BCA. Untuk memastikan proteksi komunikasi selama Anda mengakses internet banking BCA, Anda dapat melakukan hal-hal sebagai berikut:

* Periksa sertifikat SSL secara teratur untuk memastikan bahwa Anda menerima sertifikat SSL yang sah yang telah terdaftar untuk IBANK.KLIKBCA.COM.
* Apabila Anda menerima pesan yang menjelaskan bahwa sertifikat tidak sah, dimohon Anda tidak melanjutkan akses internet banking BCA.
* Pastikan bahwa Anda telah mengetik alamat yang benar yaitu <https://ibank.klikbca.com>.
* Pastikan bahwa pada browser Anda terdapat gambar gembok/kunci yang mengindikasikan bahwa halaman yang Anda akses saat ini dienkripsi dengan menggunakan SSL. Jika Anda tidak melihat gambar gembok/kunci, dimohon Anda untuk logout dan kemudian melakukan login kembali.
* Pastikan bahwa Anda telah logout saat meninggalkan komputer Anda meskipun hanya sesaat.
* Sebaiknya Anda tidak mengakses internet banking BCA di warnet atau di jaringan yang tidak pasti keamanannya.

3. Proteksi Akses Internet Banking BCA

BCA mewajibkan Anda untuk memasukkan User ID dan PIN sebelum Anda dapat melakukan akses ke internet banking BCA. Untuk memastikan proteksi bagi Anda dalam melakukan akses ke internet banking BCA, mohon lakukan hal-hal sebagai berikut:

* Jagalah kerahasiaan User ID dan PIN Anda, jangan diberitahukan kepada orang lain, kecuali untuk melakukan transaksi-transaksi tertentu yang mengharuskan Anda untuk memberitahukan User ID milik Anda, antara lain untuk transaksi pembelian barang atau jasa secara on-line, dan jangan disimpan dalam Internet Explorer Anda.
* Jangan memberitahukan PIN atau sebagian PIN Anda kepada orang lain, walaupun orang tersebut mengaku sebagai karyawan BCA. BCA tidak pernah menanyakan PIN Anda.
* Gantilah PIN Anda secara periodik di internet banking BCA pada menu Administrasi-Ganti PIN atau jika Anda tidak yakin terhadap kerahasiaan PIN Anda. Jangan menggunakan PIN yang mudah diterka seperti: 111111, 222222, 123456, 654321, tanggal lahir, nomor mobil, alamat dan lain-lain. Jangan menuliskan PIN Anda di tempat dimana orang lain dapat membacanya.
* Gunakan PIN internet banking BCA yang berbeda dengan PIN yang Anda gunakan untuk mengakses situs lain.
* Hubungi Halo BCA jika Anda lupa PIN atau PIN Anda terblokir. Ikuti instruksi mereka bagaimana cara untuk mengaktifkan fasilitas internet banking Anda kembali.

4. KeyBCA dan Proteksi KeyBCA

BCA mewajibkan Anda menggunakan security token yang dinamakan KeyBCA untuk menghasilkan One Time Password yang digunakan untuk mengotentikasi setiap transaksi finansial Anda dan sebagai tanda persetujuan Anda terhadap transaksi yang dilakukan. Anda harus memasukkan One Time Password yang dihasilkan oleh KeyBCA jika Anda melakukan transaksi finansial seperti : transfer dana, pembelian dan pembayaran dan transaksi non finansial seperti : aktivasi KeyBCA, tambah koneksi, hapus koneksi dan registrasi inquiry tagihan kartu kredit BCA Transaksi yang dapat dilakukan tanpa menggunakan KeyBCA adalah : informasi rekening, status transaksi, history transaksi, administrasi dan email Untuk memastikan proteksi bagi KeyBCA Anda, mohon lakukan hal-hal sebagai berikut :

* KeyBCA Anda diamankan dengan PINnya sendiri. Gantilah PIN KeyBCA Anda segera setelah Anda menerima KeyBCA, dan gantilah PIN KeyBCA secara periodik atau jika Anda tidak yakin terhadap kerahasiaan PIN Anda. Jangan menggunakan PIN yang mudah diterka seperti: 111111, 222222, 123456, 654321, tanggal lahir, nomor mobil, alamat dan lain-lain. Jangan menuliskan PIN Anda di tempat dimana orang lain dapat membacanya.
* Jangan meminjamkan KeyBCA Anda kepada orang lain.
* Jagalah kerahasiaan PIN KeyBCA Anda, jangan diberitahukan kepada orang lain.
* Jangan memberitahukan PIN atau sebagian dari PIN KeyBCA Anda kepada orang lain, walaupun orang tersebut mengaku sebagai karyawan BCA. BCA tidak pernah menanyakan PIN KeyBCA Anda.
* Hubungi Halo BCA jika KeyBCA Anda hilang, rusak atau terblokir. Ikuti instruksi mereka bagaimana mendapatkan KeyBCA baru atau mengaktifkan KeyBCA Anda kembali.

5. Alamat E-mail dan Proteksi Informasi Transaksi

BCA mewajibkan Anda untuk memberikan alamat e-mail Anda kepada BCA. BCA akan menggunakan alamat e-mail Anda untuk mengirimkan informasi atas transaksi finansial yang telah Anda lakukan melalui internet banking BCA dan beberapa transaksi non finansial yaitu saat login pertama kali, perubahan alamat e-mail, tambah koneksi, dan lain-lain. Selain itu BCA juga menggunakan alamat e-mail Anda untuk kepentingan promosi, undangan gathering dan informasi-informasi lainnya.

Untuk memastikan proteksi pengiriman informasi ke alamat e-mail Anda, mohon lakukan hal-hal sebagai berikut:

* Berikan kepada BCA alamat e-mail pribadi Anda. Jangan menggunakan alamat e-mail palsu.
* Ubahlah segera alamat e-mail Anda di internet banking BCA jika Anda mengganti alamat e-mail Anda.
* Jika Anda menghubungi BCA melalui e-mail, jangan mengirimkan informasi rekening Anda yang sifatnya rahasia atau sensitif, termasuk PIN Anda.

 Ancaman juga dialami oleh semua pengguna internet termasuk internet banking BCA. Oleh karena itu kami dari pihak BCA meminta perhatian Anda sebagai pengguna internet banking BCA atas beberapa jenis ancaman yang mungkin Anda temui ketika mengakses internet. Kiat-kiat pengamanan yang dapat dilakukan sewaktu Anda menggunakan internet banking BCA, adalah sebagai berikut :

1. Phising.

Phising adalah cara-cara penipuan yang dilakukan oleh pihak-pihak tertentu untuk mendapatkan informasi-informasi rahasia seorang nasabah seperti User ID dan PIN. Ada beberapa cara antara lain :

* Berpura-pura sebagai seseorang dari pihak bank dan meminta data-data nasabah dengan alasan-alasan tertentu
* Mengirim email yang berisi login screen dan meminta nasabah melakukan login dengan memasukkan User ID dan PIN.
* Mengirim email yang berisi login screen dan meminta nasabah melakukan login dengan memasukkan User ID dan PIN.
* Mengirim URL link ke situs yang dibuat semirip mungkin dengan situs resmi milik bank namun ternyata palsu.

Kiat-kiat pengamanan:

* Perlu diketahui bahwa BCA tidak pernah mengirim email seperti yang dijelaskan diatas kepada nasabah. Apabila Anda menerima email semacam itu yang kelihatannya berasal dari BCA, Anda dapat langsung menghapus email tersebut.
* Apabila Anda terlanjur mengisi informasi yang diminta atau merasa bahwa User ID dan PIN Anda sudah tidak rahasia lagi, segera hubungi Halo BCA. Pastikan situs yang Anda kunjungi adalah http://www.klikbca.com dan https://ibank.klikbca.com dan pastikan juga bahwa gambar gembok/kunci pada browser Anda utuh ketika mengakses https://ibank.klikbca.com.

2. Virus / Worm

Virus Komputer adalah program-program komputer yang dibuat dengan tujuan-tujuan tertentu. Pada umumnya virus merusak sistem operasi, aplikasi dan data di komputer yang terinfeksi. Virus dapat menyebar melalui banyak media, antara lain e-mail, disket, CD, USB drive, Flash memory, program dari internet, maupun jaringan, dan juga dari halaman situs yang ’jahat’.

Beberapa contoh dampak dari infeksi virus:

* Komputer menjadi tidak stabil dan sering ‘hang’ (macet).
* Komputer manjadi lambat.
* Data di harddisk terhapus.
* Program aplikasi tidak dapat digunakan.

Yang mirip dengan virus adalah Worm yang dibuat untuk dapat menyebar dengan cepat ke banyak komputer. Walaupun umumnya worm tidak menimbulkan kerusakan seperti virus, namun worm dapat digunakan untuk membawa berbagai macam muatan/attachment termasuk yang berbahaya.

Kiat-kiat pengamanan:

* Gunakan anti-virus ter-update di komputer Anda, dan pastikan bahwa komputer Anda di-scan secara real-time.
* Banyak virus yang datang melalui e-mail yang diterima, sehingga Anda harus lebih hati-hati pada waktu menggunakan e-mail. Hapus e-mail yang mencurigakan atau yang datang dari pengirim yang tidak dikenal, dan scan e-mail attachment sebelum dibuka.
* Gunakan firewall pada sistem operasi di komputer Anda atau instal personal firewall dan pastikan bahwa pengaturan firewall yang terpasang dapat mengamankan PC Anda.
* Sebaiknya Anda tidak mengakses atau bahkan mendownload file/program-program di internet dari situs yang tidak dikenal/tidak dapat diyakini keabsahannya.
* Scan file-file yang berasal dari disket, CD maupun USB drive yang Anda terima.
* Pastikan bahwa sistem operasi maupun aplikasi di komputer Anda sudah dilindungi dengan sistem proteksi terkini.

3. Spyware

Spyware adalah sejenis komputer program yang diprogram untuk ’mencuri’ informasi-informasi penting/pribadi dari komputer yang terinfeksi dan mengirimnya ke lokasi tertentu di internet untuk kemudian diambil oleh pembuatnya. Informasi yang menjadi target utama contohnya: nomor kartu kredit, User ID dan PIN/password, nomor rekening, alamat e-mail, dan lain-lain.

Spyware dapat terinstall melalui e-mail attachment, program yang diinstall dari sumber-sumber yang tidak jelas, ataupun oleh web site yang ’jahat’.

Virus dapat diprogram untuk menyebarkan spyware. Namun, berbeda dengan virus yang sifatnya lebih merusak, spyware bekerja secara diam-diam agar tidak terlacak sehingga lebih mudah mengumpulkan informasi yang diinginkan sang pembuat/penyebar spyware.

Kiat-kiat pengamanan:

Pengamanan terhadap spyware sama dengan pengamanan terhadap virus/worm.

4. Bot (roBot)

Bot adalah sejenis komputer program yang apabila terinstal di PC Anda, dapat menyebabkan PC Anda dikontrol oleh orang lain secara remote melalui jaringan. Sang pembuat/penyebar Bot akan dapat melakukan apa saja dengan PC Anda.

Umumnya PC-PC yang telah terkontrol (dikenal sebagai Botnet) digunakan untuk mengirim SPAM, Virus, Worm atau untuk menyerang komputer-komputer lain yang terkoneksi ke jaringan.

Kiat-kiat pengamanan:

Pengamanan terhadap spyware sama dengan pengamanan terhadap virus/worm.

1. [↑](#footnote-ref-2)