INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL

Sir M.Ovais Notes

Compiled & Presented by: *Syed Atif Hassan Abidi*

PREFACE

The Examinations of ICAP are a demanding test of student's ability to master the wide range of knowledge and skills required of the modern professionals. Subject of "ITMAC" is one of the efforts made by ICAP in this context

The notes in your hands are the class lectures of Sir M.Ovais and cover the course of ITMAC in a very precise, yet comprehensive, manner. All the topics have been arranged bullet wise covering the key points. Hopefully these notes would serve you a lot in revising the course.

Disclaimer:

Nothing in these notes has been prepared by me. I just have arranged and formatted these notes in a meaningful manner for the convenience of the students. Moreover completeness of these notes could not be ensured by me.

[Oral permission of Sir M.Ovais has been taken prior to publicizing these notes]

If you find any discrepancy or error in these notes, Please mail me by referring the relevant page number along with the mistake made therein. (syedatifabidi@gmail.com)

May ALLAH bless you with success in every exam of both lives.

Please also remember me in your kind prayers.

Thanks

Talib e Doa

Syed Atif Hassan Abidi

January, 2011

INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL

CONTENTS: **PAGE NO.**

1. INTRODUCTION TO IT STRATEGY & MAGAGEMENT

1.1 Organizational Issues – Important Points

1. CENTRALIZATION /DECENTRALIZATION

If both the storage and processing of data are being carried out at the same place on a single machine, then the system is said to be **Centralized**. While under a **Decentralized** system, the storage and processing of data are carried out by several independent computers. All Airlines are centralized but all food chains are decentralized. It should be according to business needs.

2. ROUTINE PROCESSING

Nowadays you no need to visit your customer or supplier for processing of orders, payments or collection. I.T. has saved you from these day to day hassles and has made your routine processing very simple as well as speedy.

3. CONSTANT CHANGES

There are a lot of hardware changes, a lot of software changes, a lot of Netware changes nowadays, due to rapid advancement and updating of technology even DSL internet has become an old story. Satellite internet is being used.

4. KNOWLEDGE MANAGEMENT

If knowledge is not managed properly, it becomes lost when you need it.
Two types of knowledge are:

- Explicit Knowledge (e.g. C.A.)
- Tacit Knowledge (generally people do not share it e.g. hard earned experience of my life/my articleship)

Now specialized software for knowledge management are available. IBM has "Content Management" for this purpose. SAP and Oracle has "Knowledge Management". Knowledge management softwares are different from DBM. They contain rules also alongwith the data e.g. they contain rules for allowing data also alongwith the students' data.

5. EMPLOYMENT ISSUES

Nowadays, we don't need employees without computer literacy. Even a clerk should be computer literate. Every one wants high tech employees.

6. CUSTOMER SERVICE

This concept has been newly introduced but has become too popular that has been adopted even by Government Organizations. Now you can manage your data and make queries and complaints on phone or internet. No need to visit physically. E.g. at ACCA you can create, maintain or alter your record through internet. However, ICAP you will have to visit ICAP office and submit an application form manually to incorporate any change in your record.

7. CUSTOMER RELATIONSHIP MANAGEMENT

This is something more than just customer service. The idea of CRM is to create extremely good relations with the customers. Usually adopted by banks, travels agencies etc.

8. ORGANIZATIONAL STRUCTURE

Organization today has become flatter because technology has removed the middle management. Every thing has become automated, every person has become too productive. One computer operator is replacing 5 clerks.

9. TECHNOLOGICAL EFFECTS.

Today we have new products which did not exist earlier like internet, office equipment etc. Now, we have new methods of offering products e.g. E-commerce. Its very easy, even for a small company, to business globally. Make a website and receive orders from every where in the world.

10. HOME /TELE /REMOTE WORKING

Remote working allows an employee to connect his system with his organization's network through intranet and to perform his duties while sitting at home. This can save, not only office space, but can also save employees from hassles, fatigue, time and cost of transportation.

11. E-BUSINESS TECHNOLOGY

Transactions, marketing, services all through internet nowadays.

12. DEVELOPMENT IN COMMUNICATION

Earlier international calling charges were Rs.125 per minute
Now calling rates through land line is Rs.2 per minute
This is due to rapid development of communication technology.

13. SECURITY

Now we have lot of security issues, now you are more vulnerable. Cyber Crime Law, 2006 have been introduced in Pakistan as well.
If you upload photograph of a person without his permission: an imprisonment of 6 months.

14. OPEN SYSTEM

System which can be linked up with other system, your cell phones can be linked up with all the 5 networks and land line as well.
6 networks are:

- NOKIA
- LG
- MOTOROLA
- SONY ERICSON
- SAMSUNG

15. INTER OPERABILITY

It talks about seem less in integration. Your cell phones are open system but the problem is inter operability. When you send a message from Nokia to any 5 other networks, it maintains it's inter operability and you cant detect any formatting problem due to change of network, but in case of MMS, the system loses its inter Operability and you can observe some distortion in MMS.

16. BACKWARD COMPATIBILITY

Every new thing should work with old thing whether hardware, software or NetWare. You can take print from an old printer through a latest computer. You can open an XP Office file on window 98

17. LEGACY SYSTEM

It means your old system. At times, you would have noticed that an organization is running both the old and new systems. The new system should be backward compatible with legacy system.

18. OPEN SOURCE

When you write a program in high level language (source code) then it is compiled / interpreted in machine language (object code/machine code). Supplier never provides you source code. Reverse compiling is possible but it is too difficult and also illegal.

Peter Norton is doubted to have reverse-complied the Windows

Open source is an idea to provide source code to the customer /end users. Software companies can still earn because 99% of their customers do not have expertise to modify the software. However, 1% customers comprise of institution may have such expertise, but again, these 1% institutional customers will have to consume a lot of efforts and time to modify the software. It is better for them to buy.

Thus open source softwares earn in fact increase the revenue of software companies. By the way, "LINUX" is an open source software.

Windows is the most popular but a low profile software. It has a lot of security problems. It was developed in 1995 when there was no internet.

Advantages of Open Source:

- Reliability
- Stability
- Auditability
- Cost
- Flexibility
- Freedom
- Support (Technical support)
- Accountability

19. ACCOUNTING ISSUES

You are investing a lot of money in I.T. Some banks are investing 5 million per month in I.T. Who should bear this expense?
We have 03 solutions:

1. IT as a Corporate Overhead

It implies that all the expenses on IT should be born by the head office. No cost allocation.

Advantages:

- No complexability in calculation.
- Encourage innovation because no one is being charged.
- Good relations between IT and use department.

Disadvantages:

- No cost control
- Inefficiency
- Substandard services to user department, because no one will complaint for inefficient working /system.
- No true performance picture.

2. IT charged at cost

IT cost is allocated to each user department on the basis of services received by each.

Advantages

- Realistic
- Efficiency
- Good services to user department
- True performance picture

Disadvantages

- Finding a cost unit, whether per page, per data entry or per print.
- No good relations
- Inefficiency may be passed e.g. waste pages by IS department may be claimed as test pages.

3. IT charged at market

IS department will charge its services to other user department at market rates.
(This changing is actually on books not on reality)

Advantages

- Profit centre
- High standard services, because it is being provided at market rates
- Cost cutting
- Efficiency

Disadvantages

- Administrative hassles
- No comparable services

BUT NOW DAYS WE HAVE 1 MORE WAY OF CHARGING IT COST I.E.

Establishing IT Department as a separate company

Deals it as an outside vendor

Advantages

- More skills because outsiders may also hire for different services.
- IT department becomes a profit centre
- Better career path for IT people
- Employees are retained.

Disadvantages

- Administrative hassles
- Focus is lost (earlier IT department was developing application for the banks only but now also for other business)
- No priority for parent company.

20. OUTSOURCING

To give your work to anyone

- Cheaper
- Save time
- Contracting out services to some one outside the organization, this is called outsourcing.

E.g. accounting services

Reasons

a. Concentrate on core business
b. Flat Structure
c. Flexibility
d. Profits

Classification

1. Total outsourcing
2. Partial outsourcing
3. Adhoc outsourcing (as it needs arises)
4. Project management (every kind fixed, fixed jobs, fixed period.)

Types of services / levels

1. Time sharing (to give access to another)
2. Services _____(offering many services)
    - Data entry services
    - Programming services
    - Networking services
3. Facility Management:
    - Your own resources / facilities managed by other / someone else
    - Audit department managed by audit firms
    - PIA
    - My bank

Organization involved

1. F.M. Companies. (Facilities Management)
    - SI-3
    - Saver
    - Audit firms
2. Software houses
3. Hardware vendors
4. Consultancy firms
5. Service bureau
6. ASP (Application Service Provider)

Development in outsourcing

1. Multiple sourcing
    - I do not give my work to one vendor but more than one vendors
2. Incremental sourcing
    - Do not give all jobs on day one but give little further, further
3. Joint ventures sourcing
    - Bank develops accounting software and when sold to another software Co. and bank will share in.
4. ASP (Application Service Provider)

Managing Outsourcing Contract

1. Do not outsource your strategic system.
2. Do not outsource the complex / sophisticated.
3. Isolated system are highly recommended.
4. Payroll system.

5. System requirement should be made clear.
6. Vendor knowledge.
7. Good relation with vendor.
8. Legal contract with vendor.

Contents of services level agreement / contract

1. Service level required.
    - City credit card division is outsourced.
2. Time frame.(period)
3. Exit route.
4. Priorities.
    a. accounting
    b. marketing
    c. production
5. Software ownership.
    - At the end of contract who will retain the software, it should be mentioned in contract
6. Employment issues.
    - Work forced hired, who will retain the work forced.

Advantages

- Fixed Price
- Economies of scale
- Long term contract
- Experienced work forced
- Skills are retained
- New skills availability
- Flexibility

Disadvantages

- Information in other hands
- Information / System unavailability
- Information leakage
- No Competitive advantage
- Vendor Failure is our failure
- Locked for long time
- No experience of Information Technology
- Cost may exceed expectation.

21. **IN SOURCING**

Transfer people from user department to information system department

Advantages

- Multi skills
- Employees are retained
- Business people in information technology
- Create good relations between user and I..T. department

Disadvantages

- Inability to learn new skills
- Unwilling to switch
- Replacement of transfer employee

22. Application Service Provider (A.S.P.) (Outsourcing vendor on internet / WAN)

Functions

- Own and Operate server
- Own and Operate software application
- Employ people who operate / run the system
- Service any where and every where
- Charge a nominal fee.

Advantages

- Low and no setup cost
- Pay as you go
- No specialization
- User has his own bandwidth
- Flexibility

Disadvantages

- Same as outsourcing

Serious points to consider

1. Customer access:
   - Browser for websites
   - Special browsers E.g. at Airport terminal we can use internet
2. Customer Issues:
   - Training
   - Queries
3. Secure Connection
4. Dedicated or shared application server (dedicated is recommended)
5. Problem resolution capacity
6. Level of Redundancy / backup
7. Disaster recovery
8. Date ownership
9. Data security
10. Transfer of date between In-house application and ASP
11. How to switch to another ASP.

23. NETWORK

Network is a connection of autonomous processes. Two or more processes are said to be autonomous if they can work independently with each other as well as collectively.

Our mobile phones processes do not form a network because they are not intelligent enough to work independently. Similarly if several I/O devices are attached with a super, mainframe or minicomputer, it is not a network because I/O devices are not able to work independently if they are disconnected.

However, if two or more micro computers are connected with each other and they are able to work independently as well as in a sharing network, then it is a NETWORK.

NETWARE
(SOFTWARE NEEDED TO RUN THE NETWORK)

Client – Server
One computer is server and other computer is client. The biggest example might be internet in which we are the clients of an internet ISP. Again IPSs are client of internationally recognized networking bodies. (Hyundai, AT & T, British Telecom)

Peer to Peer
No one is server, no one is client. Every machine is server and every machine is client.

4 reasons for forming Network

- Sharing of data/information
- Sharing of resources (e.g. printer, hard disk, CD drive)
- Sharing of services (e.g. internet service, stock exchange service)
- Security (You cannot take data away from the network hard disk. A lot of instructions are imposed even to access data.)

FRICKING

Trying to access an unauthorized network e.g. trying to select telenore network with Mobilink SIM, (settings/ phone settings / network selection / manual / / warid or telenore)

Now in NOKIA reminder can be set only up to the date upto which date can be set. But in samsung,, there is still an inconsistency. Another programming problem found in all mobile sets is that they do not stop users while he/she is setting a reminder to be rung on a past date.

SAP & Oracle Financials are foreign ERPs while Sidat Hyder Financials is a local one.

1.2 STRATEGY DEVELOPMENT

- General guidelines to achieve long term objectives

Strategic Planning

- Formulating
- Evaluating
- Selecting strategies

Why to make strategy

Michael Earl give 09 reasons:

- I.T. involves high cost.
- I.T. is critical to the success of organization
- I.T. is part of commercial strategy for competitive advantage
- I.T. is required in economic context.
- I.T. affects all level of management.
- I.T. has brought revolution in information creation, presentation and management.
- I.T. has many stakeholders.
- Technical issues in I.T. are important.
- I.T. requires effective management as it makes real difference.

…….Some notes Missing……

8. Programmers

9. Help desk / information centre:

- Helping users
- Providing technical support
- Problem resolution
- Suggestion for improvement
- Guidance on standards / security
- Support End User Computing (EUC)

10. Data Management

- Data architecture and managing as corporate resource

11. Database administrator (DBA)

- Creation
- Maintenance
- Safety
- Security
- Integrity of database.

12. Security administrator

- Implementing and maintaining physical and logical security as per policy

13. System administrator

- Contracting a network

- Setting up of accounts
- Installing system wise software.

14. Network manager / administrator
    - Planning
    - Implementing
    - Maintaining the telecom network

15. Librarian
    - Receiving
    - Safeguarding all programs and data files maintained / stored on tapes

16. Control group
    - Collecting
    - Logging
    - Submission of input of various user groups

17. Schedulers
    - Responsible for backups at regular intervals
    - **Lights out operations** (Automatic backup procedure by computer itself, robotic arms are used for changing tapes)

18. Data controller
    - Checking the input, process and output.

19. Operators
    - Input, process and output the data.

20. End user
    - Execute operations related to business application services.

1.3 HUMAN RESOURCE POLICIES AND PROCEDURES

Policies

Policies are guidelines which allow or restrict decision making. Policies are high level documents incorporated in the philosophy and strategic thing of management. These must be cleared, concise and in writing. Management formulates, develops, documents, promulgates and controls the policies. Management must review all policies periodically.

Two approaches of policy making are:

- Top Down (lower lever policies are derived from corporate policies)
- Bottom up (operation level policies guide the development of corporate policies)

Procedures

Procedures are derived from parent policies. These must be cleared, concise and in writing. Procedures are more dynamic than policies.

Human Resource policies and procedures

These deal with hiring, firing and promotion of staff.

1. Hiring

Control Risk

- No suitable person is available
- No reference checks done.
- Temporary / third party staff may lead to uncontrolled risk
- Lack of awareness of confidentiality requirements.

Controls

- Background check
- Confidentiality agreement.
- Employee bonding
- Conflict of interest agreements.
- Non compete agreement
- Employee handbook:
  - Security policies and procedures
  - Company expectation
  - Employee benefits
  - Vacation policies
  - Overtime rules.
  - Outside employment
  - Performance evaluation
  - Emergency procedures
  - Disciplinary action for absence, non compliance of policies and breach of confidentiality.

2. Promotion policies

It should be based on performance, fairness and understood by every employee.

3. Training policies

It has to be on fair and on regular basis. This strengths the commitment of employees and make them customer focused. Training is given in case of any updation / upgradation or any change in the job description. Cross training should be encouraged to have backup persons.

4. Scheduling and time reporting

It provides the accurate information about the efficient utilization of the resources and helps management to determine staff requirements.

5. Employee performance evaluations

I.S. manager and I.S. employees should set mutually agreed goals. Salary increment, performance bonuses and promotion should all be based on performance.

6.Required vacation (Enforced vacation)

7.Job rotation

8.Termination policies

There should be clearly defined steps of termination policy in writing. The policy should address both types of policies.

- Voluntary may be dangerous.
- Voluntary (dangerous).

Control Procedures

- Return all access keys.
- Delete log on IDs and Password.
- Notification to other staff about the terminated employee.
- Arrangement of final pay.
- Termination / exit Interview.
- Return all company property.
- Escort the person to main Gate.

1.4 INFORMATION SYSTEM MANAGEMENT PRACTICES

Four Important Points

1. **Management Principles:**

   a) People Management :- (different from other department)

   - All educated / highly qualified persons.
   - Frequent job switches. Keep shifting.
   - Flat Structures, very few people.
   - Juniors having significant roles.

   b) Management of Change:-

   - So frequent changes in IT department.
     - New Technologies.
     - New Application / Updation
   - You need to be updated.

   c) Focus on Good processes

   - We want the Best.
   - Good practices are being evolved and you have to follow these practices
     - Programming Good Practices
     - Banking Good Practices. (by SBP)

   d) Security Management**:-**

   - So many Security Threats.
     - External threats
     - Internal Threats.

Internal Users	External Users
IT department people	Students/external auditor

   - Business Continuity and Disaster Recovery:

   e) Handling Third Parties:

   - Software Vendor, Supplier, Customer are accessed your system.
   - Hardware, Software, Networking Vendors.
   - When they come in, they can access other Hardware and Software.

2. **IS Assessment methods:**

   - You have to access.
   - IS Department, IS People Performance to see deviation.

   Seven Methods of Assessing:

   a) IS Budget:

   - You must develop a Budget.

- Also Monitor Budget.
- To Calculate Variances.

b) Capacity and Growth Planning:

- Your work is increasing all the time you have to increase your capacity i.e. done during strategic planning.
- Business development and IT development should match.
- Cost Saving.
- Customers remain happy.
- Check Capacity of Hardware, Software and Networking.

c) User Satisfaction:

- Meet their requirements.
- SLAs (Service Level Agreements) are being properly enforced.
  IS department has SLA with marketing department etc.
- Periodic Audit of SLA.
- Interviews and Surveys.

d) Industry Standards / Benchmarking:

- Every industry has its own standards and we have to perform according to standards.

e) Financial Management Practices:

- Charge at cost (recommended)

f) Goal Accomplishment:-

- All goals are set by I.T. department.
- Comparing performance with goals:
  - Effectiveness
  - Efficiency
  - Economy

g) System Logs (Record):

- Should be comprehensive logging
  - Can be manual or automatic (e.g. city bank ATMs. have door lock system)

3. Quality Management:

It helps to measure, control and improve processes to produce desire results.
It includes:

- Quality assurance (setting standards and procedures)
- Quality control (checking)
- Quality Management.

Areas to be focused

- General administration
- HR management
- Acquisition of hardware and software
- Software development, implementation and maintenance
- Day to day operation
- Security

4. Performance optimization: (Maximum performance)

- Performance measurement (its dynamic process because it change every day)
- Performance measurement is becoming strategic requirement.

a) Phases of Performance Measurement (04 phases)

- Establishing and updating performance measures
- Establish accountability for performance measures
- Gathering and analyzing performance data
- Reporting and using performance information.

b) Limiting factors in performance measurement

- Lags (time log)
- Work today and know result later (ICAP result)
- Measurement error
- Mismanagement (misallocation of cost)

c) Uses of performance measurement

- Measure product / services
- Manage product / services
- Assure accountability
- Make budget decision
- Optimize performance

1.5 SEGREGATION OF I.S. AND OTHER ORGANIZATIONAL FUNCTIONS

There are following which must be segregated in I.S:

1. **Transactional authorization by user department:**

   - User department are responsible and not I.T. department
   - Periodic checks by management & auditors
   - Review should be carried out
   - Define limit of authorization

2. **Reconciliation**

   - Responsibility of user department
   - Data control room
   - Use of controls totals & balancing sheets by control group (independent verification.

3. **Custody of Assets**

   - Responsibility of user department
   - If digital (I.T. department)
   - data owner provide authorization leves for adequate security
   - data administration group responsible for implementation & enforcing security system

4. **Access to Data**

   - I.T. department grant access but permission come from user department
   - Access should be given on need to know basis
   - Controls over access to data by physical, system & application security.
   - Control from internet

5. **Authorization forms**

   - Give user information to I.T. department through forms from user department and it is kept by the I.T. department.
   - Authorized specific system access via written requests of Management
   - Access privileges should be periodically reviewed

6. **User authorization tables**

   Data of forms to build & maintain user authorization table & reviewed periodically by authorized person by data encryption.

   Forms = Access person
   Exception = should be investigated.

7. **Exception reporting**

   - User department are responsible (e.g. audit report)
   - If there is technical exception then I.S. department is responsible
   - Exception has been properly handled & Resolved in timely manner.

8. Transactional logs

- I.T. department is responsible for transaction log (record of transaction)
- Manual log e.g. record of transaction (grouped or batched) before they are submitted for process
- Automated log: by computer system.

9. Audit trail

- I.T. department is responsible
- Track for the purpose of inspection
- Use to detect fraud and error
- Component of will designed systems.
- Help IS department and auditor by flow of transaction
- Flow of transaction from initiation to end.
- IS auditor should be able to determine:
  - Who initiated the transaction
  - The time of day & date of entry
  - The type of entry
  - What fields of information it contained
  - What file it updates

1.6 I S. SECURITY MANAGEMENT

Key elements of information security management

1. **Policies and Procedures**

   a) Define importance of information assets
   b) Point out sensitive and critical assets to protect
   c) Need for security
   d) Accountability

2. **Organization**
   Responsibilities are defined by position

   a) Executive /top management

   b) Security Committee
      - Involve technical/user/executive management people, it sets guidelines, policies and procedures.

   c) Data owners
      - Determine data classification levels, maintain accuracy, completeness and integrity of management.

   d) Process owners
      - Ensure appropriate security as per policy

   e) Security specialist or advisor
      - It sets and design implementation, management and review of security policy, standards and procedures.

   f) Users
      - Read policies, follow procedures, keep log on IDs and password secretes and report violation.

   g) I.T. Developers

   h) I.S. Auditor
      - To provide independent assurance.

3. **Data classification**

   a. Data is classified by designation
   b. Access is given on need to know basis.
   c. It reduces the risk and cost of over protecting the information resources.

4. **System access:**
   The ability (read, write) to do something with the computer resources

   a) Information owner should authorize access in writing
   b) Access should be on need to know basis and documented
   c) Access rights should be periodically reviewed
   d) Two types of access:
      i. Logical: it can be blocked through operating system, application program, database system and network control devices.
      ii. All four layers should be covered
         - Platform (hardware and operating system)
         - Network
         - Application system
         - Databases

   e) Physical Access
      Control incoming and outgoing of people. Restrict physical access.

f) Proper system access management requires:

- Security awareness and education
- Monitoring and compliance
- Incident handling and reporting

5. Information security management standards

a) Privacy impact analysis (Two Parts)

- Employee privacy: Name, address, NIC No., phone No. and all details should not be disclosed to anyone.
- Consumer privacy: business organization should not disclose their customer details to anyone (e.g banks know all details about its customer)
  - i. Right of subject
  - ii. Laws and Regulations
  - iii. Transaction border data flow:
    - Data travel from country to country. You have multiple jurisdiction
    - Involve experts from operations, legal, technical and marketing side.

b) Critical Success Factor (CSF) for I.S. management and security

i. Senior management involvement
ii. Developments of I.S. security policy
iii. Updating of security policy and procedures

6. Computer crimes, issues and exposures (White color crime)

i. Threats

a) Financial loss
b) Legal repercussion /consequences
c) Loss of credibility
d) Blackmailing
e) Industrial espionage (Industrial spy)
f) Disclosure of confidential, sensitive or embarrassing information
g) Sabotage

ii. Perpetrators

a) Hackers (They gain unauthorized access)
b) Employees (both authorized and unauthorized)
c) Former employees
d) I.S. personnel
e) End user
f) Interested /educated outsiders
   - Competitors
   - Foreigners
   - Organized criminals
   - Students
   - Crackers (paid hackers)
   - Freekers
g) Part time and temporary personnel
h) Vendors and consultants
i) Accidental ignorant

2. CONTROLS

2.1 ENVIRONMENTAL EXPOSURE AND CONTROL

- **Issues and Exposures**

a) Power failure:
   - Blackout
   - Brown out (low voltage)
   - Spites and surges (voltage 220 to 440 suddenly high voltage)
   - Electro magnetic interference

b) Water
c) Fire
d) Air conditioning
e) Humidity
f) Dust
g) Food

- **Environmental Controls / Solution**

a) Power failure
Surge protectors, UPS, generators, multiple phases, emergency power off switch, concealed wiring.

b) Water
- Detectors

c) Fire
- Smoke/fire detectors, fire alarm, extinguishers, fire suppression system, halon gas, carbondioxide, fire proof material, inspection by fire department.

d) Air Conditioning
- Backup Air condition

e) Dust
- Dust controlling

f) food
- No food permission in I.T. department
- Strategically locating computer room
- Documented and tested emergency evacuation plans.

2.2 PHYSICAL ACCESS EXPOSURES AND CONTROL

Physical access Issues and Exposures

- Unauthorized entry
- Damage
- Vandalism/Sabotage (Strikes)
- Theft
- Copying or viewing of sensitive data
- Alteration of sensitive equipment and information
- Public disclosure of sensitive information
- Abuse of data processing
- Blackmailing
- Embezzlement

Physical access Controls

- Security guards
- Bolting/secure door locks
- Combination of door locks (multiple kinds of locks)
- Electronic doors
- Dead man door (e.g. Bank lockers, only one person can enter at one time)
- Controlled single entry point
- Alarm system
- Manual logging
- Electronic logging
- Identification
- Video cameras
- Secured report distribution carts
- Bounded personnel (fixed the people to enter)
- No advertising of sensitive location
- Computer workstation

PERSONAL COMPUTER /LAPTOPS PHYSICAL AND LOGICAL SECURITY

- Engraving the company name
- Logging of serial numbers
- Physical locking (e.g. IBM steel hangers)
- Theft response team
- Backup of data
- Password on files
- Data encryption

2.3 LOGICAL ACCESS EXPOSURES AND CONTROLS

I. Logical Access Issues and Exposures

Intentional or unintentional implementation /modification of data and software

a) Trojan horse
Unauthorized codes hidden in authorized code, e.g. pictures contain unauthorized data)

b) Rounding down
Round off the figures, e.g. actual figure is .039, you round it to 0.34, the difference amount is automatically transferred to programmers bank account

c) Salami technique
In this technique you round the figure to zero, e.g. actual figure is 1234.39, round it to 1234.00

d) Viruses
Self replicating code; It slow down your machine (80,000 viruses definition)

e) Worm
Does not replicate (duplicate) itself and spread through network

f) Time bombs
Does not replicate itself, explore/activate at a certain time

g) Logic bombs
Does not replicate itself, explodes/activate at a certain event

h) Trap doors
When a programmer makes a program, he keeps the trap doors, now he can modify, change the programs; e.g. cheat codes in games

i) Data leakage (Steal the data)

j) Wire tapping (cross talked)

k) Piggy backing
You piggy back you unauthorized packet of data with authorized packet of data and you can enter into the system when it allows to enter the authorized packet in the system.

l) Computer shutdown
Remote computer shutdown though a software

II. Paths for logical access

a) Network connectivity
b) Remote access (VAN)

III. Logical access control software

- It is operate in the operating system
- It may be in data base / Programmes

Function:

a) User identification (log on IDs) and authentication (password)
b) Apply restrictions
c) Create or change user profiles/setting
d) Create accountability (record each and every thing)and auditability(audit of record)
e) Log events
f) Log user activities
g) Report capabilities e.g. message in window XP don't send

IV. Identification and Authentication (Internal Audit System)

Process of providing one's identity its first line of accountability

Identification and Authentication system based on three things:

a) Something you know (log on IDs and password)
b) Something you have (ID card)
c) Something you are (By matrices)

Identification and Authentication system Examples:

a) Logon IDs and password
b) Token devices (video games)
c) One time password
d) Bi matrix
   - Thumb prints
   - Finger prints
   - Palm readers
   - Hand geometry
   - Iris checking
   - Retinal imaging
   - Facial imaging
   - Signature recognition
   - Voice recognition

e) Single Sign On (SSO)
   - Multiple password for every server
   - One password and you have access to every servers, its most dangerous (MSN Messenger)

V. Security Bypass features

- Physical example: entry is blocked; Bypass due to influence, position, special privilege.
- Bypass should be disabled for everyone**.**

Features to be considered

a) Label processing, Bypass off; label process on

b) Special system log on IDs
every system has logon IDs when you install window as administrator and then other IDs are guest users i.e. called special system logon IDs, this should be disabled.

c) System Exists
This should not be available to user; complex maintenance task/tailoring:
there are thing which cannot be recorded by system e.g. in cell phone removing battery or sim system cannot record it.

VI. Viruses

Antivirus:-

a) Scanner do scanning for signatures, every virus has its own signature/definition.
b) Immunize it will clean, detect and protect your system from the viruses

2.4 NETWORK INFRA STRUCTURE SECURITY

I. Controls in network environment

a) Qualified people are hired for networking
b) Segregation of duties
c) Restriction on important function
d) Terminal identification file (when you log on/off)
e) Encrypted transmission. Data has to be encoded

II. LAN (Client Sever) Security

i. Risk associated with LAN
   a) Loss of data and program integrity
   b) Viruses
   c) License issues
   d) External access (outsiders may access LAN)
   e) Illegal access (hackers may access LAN)
   f) Destruction of auditing and logging data

ii. Controls of LAN
   a) Dial/call back modems
   b) Turn off call forwarding (first goes to specific no.) or divert on terminal (direct goes to another no.)

III. Internet threats and security

a) Threats
   - Viruses
   - Hackers

b) Security
   - Antivirus
   - Dial back mechanism, firewall

IV. Types of network attacks

i. Passive attacks

Get knowledge before going for active attack)

Three methods of passive attack:

a) Network analysis
   - Scan operating system, services and ports/software ports (monitoring operating system)
   - Ports (Software Port) e.g. http port

b) Eaves dropping (wire tapping)
c) Traffic analysis
   - look at nature of traffic flow, means audio, video, graphic, session length (data packets)
   - message length and
   - frequency of packets)

ii. Active attacks

Five methods of active attack:

a) Brute force attack (try out all possible combinations of passwords; deadly attack)
b) Impersonation /spoofing /masquerading
c) Packet replay (you copy packet & replay it and join it with your packets and gain access to the system)
d) Email bombing
e) DOS - DDOS (Denial of service - Distributed DOS)
   - DOS: e.g. one student ask all question; Huge email
   - DDOS: e.g. distribute questions among the students

- Engaging the server (Huge email; server busy)
- Bouncing back all request (request does not reach to server)
- Blocking a specific user (block one specific user)

V. ENCRYPTION / CYAPHERING / CODING

Converting plain text into secure coded form, it is used for protecting data:

a) In transit
b) Stored on computers
c) Deter and detect accidental or intentional alteration
d) Verify authenticity

Two types of cryptography (knowledge of encryption) system

a) Private Key cryptography system (same key is used for coding and decoding)

Two systems here, for Private Key encryption:

- DES (Data Encryption Standards)
- AES (Advanced Encryption Standards)

Problem:
We need to be aware of the key. Two parties needed to share same keys. Problem arises when you communicate outside the organization.

b) Public Key cryptography system (different key is used for coding and decoding)

Encryption	Decryption
Public	Private
Private	Public

There are some CAs (Certified Authorities) who give you the private and public keys of the organizations. For example:

- CERTO
- Veri-sign
- Degi-sign
- NIFT

Objectives

- Security / Confidentiality
- Authentication (confirmation who send) & Non-repetition

Examples of Public key

a) PEM (Privacy Enhanced Mail)
b) PGP (Privity Good Privacy)
c) SET (Secured Electronic Transaction)

Objectives

a) Security / Confidentiality
   i. Encrypt: Public Key
   ii. Decrypt: Private Key

b) Authentication and Non repudiation /Digital signatories
   - Encrypt: Private Key
   - Decrypt: Public Key

If Both Objectives Are Required To Achieve Sequence Must Be (b) and (a)

VI. FIREWALL SECURITY SYSTEM

Firewall is a combination of hardware and software build using routers, servers and variety of software installed at the meeting point.
These are used to:

a) Block access to particular sites
b) Prevent user from accessing certain servers/services
c) Monitor communication between internal and external network
d) Encrypt packets

Three types of firewall

a) Router packet filtering firewall
- Accepts only authorized packets

b) Application firewall
- Built in the operating system and application system

c) Estate full inspection firewall
- Keeps the track of destination IPs to accept data from that IPs only otherwise reject the request from other IPs.

VII. IDS (INCLUSION DETECTION SYSTEM)

An IDS inspects all inbound and outbound network activity and identifies suspicious patterns. These are several types of IDS.

Types of IDS

a) Misuse detection system
- The IDS analysis the information it gathers and compares it to large databases of attacks signature.

b) Anomaly Detection (Abnormal Detection)
- System administrator defines the baseline /normal state of the networks traffic load breakdown, protocols and typical packet size. The anomaly detector monitors network segments to compare their state to the normal baseline and look for anomalies.

c) Network based system
- Detects individual malicious packets flowing through the network that are designed to be overlooked by a firewall.

d) Post based system
- Examines activities on each individual computer or host.

e) Passive system
- Detects a potential security breach, logs the information and signals and alert.

f) Reactive system
- Responds to the suspicious activities by logging off a user or re-programming the firewall.

The Difference between IDS and Firewall

Firewall	IDS
They are installed at meeting point	They are installed in your server
Check only out bound activities	Check both inbound and out bound activities.

2.5 APPLICATION CONTROLS

A. Input Control
B. Processing Control
C. Output Control
D. Storage Control

A. Input / Origination Control

i. Input authorization method

a) Signatures on batch forms
b) Source documents
c) Online access control
d) Unique password
e) Terminal / workstation identification

ii. Batch control and balancing

a) Types of batch control
- Total documents
- Total item
- Total monetary amount
- Hash total (Receipt serial no. total)

b) Types of batch balancing
- Batch register
- Control accounts
- Computer agreements (manual calculation agree with computer calculation)

iii. Error reporting and handling method

a) Rejecting only transaction with error
b) Rejecting the whole batch
c) Accepting batch in suspense
d) Accepting batch and flagging error transaction

iv. Input control techniques

a) Transaction log
b) Reconciliation of data
c) Documentation
d) Transmittal log
e) Cancellation of source document
f) Error correction procedures

- Logging of errors
- Timely correction
- Validity of correction
- Approval of correction
- Upstream resubmission
- Suspense file
- Error file.

B. Processing control procedures

i. Validating & Editing Controls

a) Sequence Checking
b) Limit Check (e.g. upper and lower limit)
c) Range check
d) Reasonableness check
e) Table lookup
f) Completeness check
g) Duplicate check
h) Logical relationship check (e.g. Mr. Mrs. Miss)
i) Validity check
j) Check digit

ii. Processing Control Procedure

a) Editing
b) Manual recalculation
c) Run to run totals (running balance)
d) Program controls
e) Reasonableness verification of calculated amounts
f) Limit checks on calculated amount
g) Reconciliation of file totals
h) Exception reports

C. Output controls

a) Logging and storage of negotiable sensitive and critical forms in a secured place.
b) Computer generation of negotiable instruments, forms and signatures.
c) Careful report distribution
d) Balancing and reconciling
e) Output report retention
f) Acknowledgment
g) Output error handling

D. Storage /Data file controls

a) Before and after image reporting.
b) Maintenance error reporting and handling
c) File updating and maintenance authorization
d) Source document retention
e) Internal and external labeling
f) Version usage (using correct and current version)
g) Data file security
h) One for one checking
i) Transaction log
j) Controls for transaction integrity in a database

- Atomicity (if transaction is either completed entirety or not at all)
- Consistency (all integrity connections in the database are maintained.)
- Isolation (each transaction is isolated from other transaction)
- Durability (transaction should survive hardware and software failures)

3. BUSINESS CONTINUITY PLANNING (B.C.P.) / DISASTER RECOVERY PLANNING (D.R.P.)

Phases of Business Continuity Planning:

1. Business impact analysis (BIA)
2. Developing business recovery strategies
3. Develop detailed plan
4. Implement plan
5. Test an implemented plan

1. Business impact analysis (BIA)

Understand the key business processes and key IT infra structure.

Two approaches
- Questionnaire
- Interviews

Three important questions:

a) What are critical information resources related to organization's critical business processes? (is it your server, hardware or software)
b) What is the critical recovery time /period for information resources?
c) What is the system risk ranking (some are very risky or low risky)

Four ranking

i.	Critical system	[Need to be replaced by identical capabilities]
ii.	Vital systems	[Can be performed manually for a brief period of time at high cost]
iii.	Sensitive system	[Can be performed manually for extended time period at tolerable cost]
iv.	Non critical system	[Can be performed manually for extended time period at litter or no extra cost.]

2. Developing business recovery strategies.

a) Criticality of business processes
b) Cost
c) Time required to recover
d) Security

Types of strategies /recovery alternatives

a) Reciprocal agreement with other companies
Agreement with two or more organizations with similar equipment or applications (it is inexpensive but difficult to reinforce)

b) Duplicate information processing facilities (IPF)
Dedicated self developed recovery sites that can backup critical applications. (Banks have done it)

c) Hot sites
Fully configured and ready to operate within several hours. Installed with low power processor to take care of critical applications. Additional needs are staff, programs, data files and documentation.

d) Worm sites

Partially configured usually with network connections and selected peripheral equipments such taps and disk drives.

e) Cold sites
Equipped with basic facilities only like electrical wiring, air conditioning and flooring.

3. Developing a detailed plan

Following factors must be considered.

a) Pre disaster readiness
b) Evacuation procedures
c) How to declare a disaster
d) Identification of business processes and IT resources that should be covered
e) List of steps required to maintain critical business functions
f) Configuration of building facilities like desk, chairs, telephones sets. Etc.
g) Step by step explanation of recovery operation
h) Identification of resources required for recovery
i) Management and user involvement
j) Consider the entire organization
k) Identification of responsibilities in the plan

Organization and Assessment of Responsibilities

a) Emergency action team (first team who does evacuation)
b) Damage assessment team (assesses damage and estimates time for recovery)
c) Emergency management team (coordinates the activities of all other teams)
d) Emergency Operation team (manages system operations at recovery site)
e) Transportation team (locates a recovery site if not determine and coordinates the transportation of employees to disaster recovery sites)
f) Network recovery team (re-routes wide area voice and data communication traffic)
g) Communication team (establishes a user/system network solicits and installs communication hardware)
h) User hardware team (coordinates the delivery and installation of user terminals, printers, typewriters, photocopies and other equipment)
i) Software team (restores system packs loads and tests operating system)
j) Application team (restores user packs and application programs on the backup system)
k) Security team (monitors the security of system and communication links)
l) Off site storage team (obtains packages and shifts media and records to the recovery facilities)
m) Data preparation and records team (updates the application database.)
n) Administrative support team (serves as a message centre for the user recovery site.)
o) Supplies team (coordinates supply of necessary office and computer supplies)
p) Salvage team (manages the relocation project)
q) Relocation team (Coordinates the process of moving from the backup site to a new location or to the restored original location)

4. Implement Plan
Implement as per details mentioned above.

5. Test and maintain plan / Test an implemented plan

i. Test execution (three phases)

a) Pre test
Set of action necessary to set the stage for the actual test.

b) Test
Real action of the business continuity test. Actual operational activities are executed to test the specific objectives of the business continuity test.

c) Post test
Clean up of group activities

ii. Types of test

a) Paper test (paper walkthrough of the plan)
b) Preparedness test (localize version of a full test)
c) Full operational test (it is one step away from an actual service disruption)

iii. Documentation of result/observations

Documentation of observations, problems and resolution

Result analysis

a) Time (elapse time for completion of prescribed test.)
b) Amount of work performed at backup site
c) Count no. of vital record successfully carried to the backup sites and no. of critical systems successfully recovered.
d) Accuracy of data entry at the recovery site.

iv. Plan maintenance

a) Changes in the business strategy
b) New application
c) Changes in the IT infra structures
d) As per environment
e) Any mishap.

4. E-COMMERCE

1. E-Commerce (Outlay buying and selling)
2. E-Business (Much broader and includes every business activity)

Steps on Getting on Internet

(i) Upgrade customer interaction
- Start doing emails
- Make a web site

(ii) Understand the customer segments:
- Wealthy
- Youngsters
- Educated

(iii) understand service process
- How many processes do we have?
- All the computerized or manual

(iv) Define the role of live interaction. Some products are bought through live interaction: e.g perfumes, cars, cloths etc.

(v) Technology decide
- Zero touch (It has no human interaction)
- Low touch (It has human interaction)

(vi) Deal with tidal waves

(vii) Create incentives and disincentives (eg. Online shopping , cash transaction)

(viii) Decide on channel choice

(ix) Explode the internet (offer them something)

(x) Implement (execute the plan made)

E- Commerce Models

1. B2B - Business to Business

a) Co. Alliance [To equal people- one buyer one seller]

b) Value Alliance [Many people / Many Business]

c) Market Alliance [One market, all people / business linked-up]

d) Star Alliance [One dominating and other linked up]

2. B2C - Business to Consumer

a) Direct customer

b) Dot Com e- tailors
e.g. msn.com

c) Bricks & Clicks e- tailors
They are people selling through manual & through internet

d) Portals (Website of Website)
Lets no advertise individual shops instead advertise shole market e.g. Tariq Road , Jinnah Super marker

e) E- Market Place
e.g Sunday Bazar

3. **B2E - Business to Employees**

4. **B2G - Business to Govt**

5. **C2G - Citizen to Government)**

6. **G2C - Government to Citizen**

7. **X2X - Exchange to Exchange**

Customer Service the Web

a) Security / Trust
b) SITE Effectiveness
c) Good Response Time
d) Response Quality
e) Download Quality
f) Navigability
g) Fulfillment
h) Up-to-Date
i) Availability
j) Opportunity
   - EDI (electronic data inchange)
   - Information connection
   - Click Stream
   - Distribution
   - Big Market
   - Virtual Supply Chain
   - Virtual company
   - E- Marketing

k) Differences In Traditional & Electronic Business
   - No / Fewer Intermediaries
   - Economies of Information
   - New networks of Communication
   - Level of speed
   - New intermediaries
   - New business partnership
   - Transparent prices
   - Dynamic prices
   - Personalize attention
   - New market segments
   - Complementary channels

ELECTRONIC PAYMENT METHOD

a) Smart cards
b) Credit / charge / debit Cards
c) Online banking
d) Digi – Cash / E- Cash
e) E- Cheque
f) E- Wallets
g) Financial Electronic Data Interchange **(FEDI)**

SECURITY SOLUTION

1. Secure Socket layer
2. Secure http
3. SEPP (Secured Electronic Payment Protocol)
4. ECML (Electronic Commerce Modeling Language)
5. SET (Secured Electronic Transaction)
6. Digital Transaction
7. EMB (Euro-pay Master Visa)

ADVANGES OF E- COMMERCE

1. Faster & Standard EDI
2. Reduce Transaction Cost
3. No / Few Intermediaries
4. Decrease Use of Cash
5. Personalize Marketing
6. Connectivity
7. Tele commuting / Tele working
8. Communication Cost
9. Faster Excess the Data / Information

DISADVANTAGES OF E- COMMERCE

1. Lack of Trust
2. Confidentiality
3. Integrity
4. Connectivity / Availabilities
5. Profit
6. Authentication and Non Repudiation
7. Power to Customer
8. Taxation
9. Legal Jurisdiction
10. Linked with Existing Business Process
11. Variety of Technical People

5. SOFTWARE

5.1 SUPPLY CHAIN MANAGEMENT:

It includes links from producers to re-seller/distributors, dealers, wholesalers, stockers, retailers and customers. It means streamlining the bus, process transaction, functions and resources. All the facilities and departments should be networked. SCM is beneficial for the organization with vertical integration (procedures – suppliers – customers)

Phases of SCM

1. **Departmentalized Organization**
   - Departments work in isolation, no good relations with trading partners

2. **Integrated Organization**
   - Departments are processes are streamlined.

3. **Integrated Supply Chain**
   - Partners are integrated and streamlined

4. **Extended Enterprise**
   - Vertical enterprise, transparent data flow.

5. **Process involved in SCM**

   i. Order entry

   ii. Warehouse management
      a) Automatic data capturing,
      b) receipt and dispatch of goods; and
      c) effective inventory management

   iii. Manufacturing Resource Management
      a) Just in Time {JIT} ,
      b) Web based ordering)

   iv. Financial Consideration
      a) Immediate preparation of financial statements
      b) Prompt payments

   v. Reduction in timeframe involved in SCM software
      a) Executioner timeframe (e.g. Order update, from days to seconds)
      b) Operational timeframe (e.g. Order fulfilling, from weeks to days)
      c) Tactical timeframe (e.g. Lead time, supplier contract term, from month to weeks)
      d) Strategic timeframe (new plant, new product, new centre, from years to months)

6. Parts of SCM software

a) SCM planning software

a) Manual management
b) Multiple facility planning
c) Production planning (scheduled)
d) Distribution / Replenishment planning
e) Transportation planning
f) Reduce inventory levels

b) SC execution software (It automates ordering, It has four things)

a) Availability premises
b) Warehousing
c) Transportation management
d) Handling International Trade
   - Documentation
   - Cost calculation
   - International laws

c) SC process management

Features
a) Forecasting
b) Collaboration (multiple people can work together)
c) Optimization (Based on linear programming)
d) Real time execution
e) Process management (work flow management [we have all departments]
f) defined by system
g) Performance analysis [all kinds of report]
h) Documentation

Suppliers of SCM

1. SAP
2. Oracle
3. Bann
4. MFG Pro
5. JD Edward

5.2 Enterprise Resource Planning (ERP)

To plan each and every thing is an organization. ERP is single integrated software that runs on single database. It integrates the information used by all level of management/ departments.

1970	MRP	(Material Requirements Planning). There is issue of capacity planning
	MRP2	It includes material + capacity planning
1980	ERP	Automated planning of each and every thing.

Reasons:
(i) Technical solution
(ii) Strategic solution (to support future strategies & having a single comprehensive view in a large organization)

ERP implementation affects

a) Business development
b) Operational development
c) designing business process
d) System development (your I.T. infrastructure is affected.

Latest Trends in ERP
1. S.M.E. / S.M.B. (Small and Medium Enterprises)
2. Modular approach
   Software in Module
   - Financials
   - Operations
   - Costing
   - Etc
3. Industry solution
4. Supply chain management
5. E-business, E-commerce
6. Outsourcing
7. Non-monolithic (from one suppler)
   Financial – Oracle
   HR – SAP

4. Important Points to Consider (ERP)
(i) Top management style
   - Centralized
   - Decentralized
(ii) Implementation time (takes one year to five years)
(iii) Technical issues
(iv) Currencies
   a). Tax rules
   b) Vendor supports
   c) Cost (implicit / Explicit)

Advantages of ERP
1. Standardized and fastest working.
2. Better information flow.
3. Integration.
4. Cheap development.
5. Safe cost estimation.
6. Know how
7. Flexibility.

Disadvantages of ERP
1. Consultant limited knowledge
2. External involvement
3. Changes in working style.

5.3 CUSTOMER RELATIONSHIOP MANAGEMENT (CRM)

It deals with the organizational and technical changes to be customer centered.

The objectives of CRM are

1. Know the customer
2. Attract new customers.
3. Make existing customers happy.
4. Solve customers problems
5. Offer products and services meeting customers needs.

Components of CRM

1. Marketing automation.
2. Profiling (complete customer profile)
3. Personalization (just as per customers)

Telemarketing (calls coming in for so many peoples)

E-mail marketing
Campaign management (whole campaign can be done and automated.

1. **Sales Automation**
   - Sales campaign management
   - Call management
   - Contract management
   - Advertisement management
   - Sales force automation
   - Accounts management
   - Pricing

2. **Service and service procurement**
   - Email response
   - Automatic call distribution.
   - Computer telephone interchange (CTI)
   - Interactive voice response (IVR)
   - Problem resolution system
   - Work force management

3. **Customers self service**
   - Web based searching
   - Interactive chat
   - Email
   - Conferencing.
   - Call me
   - Browser and application sharing.
   - VOIP (Voice Over Internet Protocol)

4. **E-Commerce**

CRM APPLICATION /SYSTEMS

1. Customers facing application (People contact the customers)
   a) contact center
      - Telemarketing
      - Tele sales
      - Tele service
   b) sales force automation
      - Managing leads and prospects
   c) field service automation
      - Service orders
      - Service contracter
2. Customer Touching Application
   Application contact the customer

      - Sales campaign management
      - Ecommerce
      - Self service customer support..
        Eg. Production information, Service request, Mange information about themselves.
      - Customer centric intelligence application (decision support capabilities to improve effectiveness efficiency of CRM)

   a) Data warehousing
      Collection of database eg. NADRA)

   b) Analytical application
      - Produced statistics – projections.
      - Pattern recognition.
      - Rcognise customer behaviour.

   c) Reporting
      Produced report.

Features to look at

- Functionality as per business.
- Single and consistent customer views.
- Integrated accessor touch point.
- BE customer contact.
- Technical change involve.
- Incremental.
- Careful selection software.
- Supplier claims.

Impact of CRM

- Increased revenues
- Increased market share
- Increased complexity.
- Multiple channel.
- Multiple technology.
- Change in beliefs.

5.4 Sales Force Automation SFA

System at automate organize and task selling process.

A: Stages of SFA

1. **Transaction Centric**
   Basic level, test about customer and prospect and managed sales in pipeline.
2. **Sales connectivity**
   Connect SFA with marketing customer service installation and service process.
3. **Knowledge and empowerment**
   Selling and selling channel related knowledge.

B: Data Mapping

It deals with data flow from the prospective customer to the right person in the organization. The details are deleted to lead and the progress of the deal till the time sales are realized.

C: Mobile service of SFA

i) Mobile phones.
j) Laptop and hand held devices.
k) Contact management system PDA

D: Results of SFA

a) Customer efficiency, effectiveness and productivity.
b) Improve customer interaction.
c) Streamline business process.
d) Improved return on SFA investment.
e) Improve customer management.
f) Rapid accurate and inexpensive communication.
g) Easier information access.
h) Reduce error and cycle time
i) Improved sales callplacing, reporting and sales scheduling.

6. IT CONTROLS FRAMEWORKS

1. **COBIT** Control Objective on Information and related Technology by ISACA (Information System Audit and Control Association)

2. **SAC** System Accountability and Control by IIA (Institute of Internal Auditors.)

3. **COSO** Committee of Sponsoring Organization of tradeway commission internal control integrating framework.

4. **SAS** Statement of auditing Standards by AICPA (American Institute of Certified Public Accountants)

5. **SYSTRUCT** & WebTrust by AIPA & CICA (Canadian Institute of Chartered Accountants)

6.1 General Framework , 7 Objective

1. Effectiveness, efficiency and economy in operation.
2. Reliable financial reporting.
3. effective control of system design
4. IT asset safeguarding.
5. Compliance with applicable rules & regulations.
6. System reliability
7. Data integrity

1. **Effectiveness, Efficiency Economy**

   - IT strategy
   - Budgeting
   - Measuring effectiveness.

   a) System quality
      - Response time (How quality system report)
      - Turned around time (I/O time)
      - Ease log information
      - Quality of documentation
      - Ability to integrated with other application

   b) Information quality

   c) Task Completion
      - Decision accuracy
      - Decision confidence
      - Decision effectiveness
      - Time taking in decision making
      - Check satisfaction.

2. **Reliable Financial Reporting**

   a. No GIGO (Garbage In Garbage Out)
   b. Information as per needs.
   c. No inter department disagreement.

3. Effective Control of System Design.

a. Build controls during development
b. Use bail approaches for designing.

Weber suggest six development approaches

1. SDLC (System Development Life Cycle).
2. Socio Technical design approach. (System should be as per the people and technical strong)
3. Political approach (Try to satisfy maximum stakeholder)
4. Soft system methodology – based on the assumptions of learning and action.
5. Prototype approach – Make a working mode of system.

Phases of Development

1. Requirement specification.
2. Analysis of existing procedure / processes
3. Acquisitions and development of solicitor
4. Testing
5. Implementation and control roll out
6. Maintenance.

4. IT Asset safeguarding

- Suitable equipment and acceptable life span
- Protection against all threats.

5. Compliance

- Quality
- Changed process
- Security process
- Education of uses
- Control of completeness, accuracy, timeliness, consistency, compatibility, authorization.

6.2 COBIT (Benchmarking nowadays as security and control process)

It is used by three parties:

1. Management (to balance risk and control)
2. Users (To obtain security and control assurance)
3. Auditors (To substantiate opinion)

CONTROL

Organization structure design to perform reasonable assurance that business objective will be achieved and undesired events will be prevented, detected and corrected.

IT control objective

Statement of the desire result or purposes to be achieved by implementation control procedure in a particular IT activity.

IT Governance

Structure of relationship and process to direct and control the enterprise in order achieve the enterprise goals by adding value by balance risk v/s return over IT and its purpose

Control objective in COBIT

- Effectiveness.
- Efficiency
- Confidentiality
- Integrity
- Compliance
- Reliability and information

IT RESOURCES IN COBIT

1. Data
2. Application system (Manual and programmes)
3. Technology (hardware)
4. Facilities
5. People

THERE ARE SIX DOCUMENTS IN COBIT

1. Executive summary of COBIT framework
2. COBIT framework.
3. Control objectives
4. Audit guidelines
5. Management guidelines.
6. Implementation tools

COBIT frame work

COBIT framework has 34 high level control objectives and four domain

1. Process: Series of joint activities protect with natural
2. Domains: Process group to gather

3. There are four domain:
    - Planning and organization
    - Acquisition and implementation
    - Delivery and support
    - Monitor

Planning and organization

It covers strategy and tactics.

- Define a strategic plan
- Define the information and architectures.
- Define technical direction.
- Define the IT organization and relations.
- Manage IT investments.
- Communicate management aims and direction.
- Manager Human Resource
- Insurance Compliance with external requirement.
- Assess Risk
- Manage project.
- Manage quality.

Acquisition and Implementation

- Identify automated solution.
- Acquired and maintain application software.
- Enquire and mainframe technical infrastructure.
- Develop and maintain procedures.
- Install and accredit (certified)
- Manage the changes.

Delivery and support

It includes the actual processing of data by application:

- Define and manage service level
- Manage third parties services
- Manage performance and capacity.
- Insure continuous services.
- Insure system security.
- Identify and allocate cost.
- Educate and train users.
- Assist and advice customers.
- Manage the configuration.
- Manage the problem of incidence.
- Manage data.
- Manage operations.

Monitor

It includes management oversight of two organization.

- Monitor the process.
- Assess internal control adequacy.
- Obtain independent assurance**.**
- Provide for independent audit.

COBIT AUDIT GUIDANCE

Requirements

1. Define the audit scope.
2. Identify the information requirements.
3. Identify the inherent risk as well as overall level of control in business process.
4. Select process and platform to audit.
5. Set audit strategy.

COBIT MANAGEMENT GUIDELINES

- Control according to the steps.
- Continuous improvement.
- Part benefit analysis.
- Bench marking – compared with others (where are you)
- COBIT offers followings:
    - CSF
    - KPI
    - KGI
    - MUA

CSF Critical Success Factors:

Most important objectives if you don't do it then, die without following points:

a. IT governance focused on enterprise goals and strategic invites.
b. IT governance focused on enterprise goals and strategic initiatives.
c. IT governance activities define with clear purpose, documented and implemented.
d. Efficient and optimal use of resources.
e. Improve effectiveness of IT process.
f. Sound oversight, control environment / culture and risk assessment.
g. Define control practices.
h. Smooth problem, change and configuration management.
i. An audit committee to oversee IT audit.

II Key performance Indication (KPI)

a. Improved cost efficiency of IT process.
b. Increase numbers of IT action plans for process improvements.
c. Increase use of IT infrastructure.
d. Increased satisfaction of stakeholders.
e. Increased staff production.
f. Increased availability of knowledge and information.
g. Increased image between IT enterprise government.
h. Improved performance measured by IT balance score card.
i. Improved performance measured by IT balance score card achieved a balance between lad and lead indicators that need to be focused on to make things happens in any IT company.

III. Key Goal Indicators (KGI)

a. Enhance performance and cost management.
b. Improved ROI on IT investment.
c. Improved time to market.
d. Increased quality, innovation and risk management.
e. Appropriately integrity standardize business processes.
f. Reaches new and existing customers.
g. Availability of appropriate bandwidth computer of customers.

h. Meeting requirements and expectations of customers.
i. Adherence to law, regulation industry standard and contractual commitment.
j. Transparency our risk taking as per risk people.
k. Bench marking comparison of IT governance maturity.
l. Creation of new service delivery channels.

Maturity Model (MM)

Maturity Model is method for evaluating and measuring of the maturity of IT governance.

MM: **New Existence:** Complete take of any recognizable processes.

1. **Initial**
   - Evidence of recognition of IT governance.
   - No standard process.
   - Approach is applied on case to case basis.

2. **Repeatable but intuitive.**
   - Global awareness of IT issues.
   - Performance indicators are under development.
   - Active senior management.
   - Individual drives the governance process.
   - Limited governance process and tools.

3. **Define Process**
   - Standardize and documented procedure.
   - Training.
   - Tools and being standardize.
   - IT balances score cards develop.
   - Root cause analysis occasionally applied.

4. **Manage and measurable**
   - Full understanding of IT governance
   - Training.
   - Clear responsibilities.
   - IT process aliens with business process.
   - Risk awareness.
   - Root cause analyses standardize.

5. **Optimize**
   - Advance and forward looking IT governance.
   - Training and communications.
   - Best practice.
   - Root cause analysis and action.
   - Extensive, integrated and optimized automation.
   - Enterprise governance and IT governance strategic linked up.

6.3 SAC, COSO, SAS & SYSTRUCT

1. System Accountability & Control (SAC)

The SAC report defines the system of internal control and describe its components provide several classification of control, describe control objective and risks and define the internal auditor role.
It provides guidance our using managing and protecting IT resources and discuss the effect of the end user computing.

Telecommunication and emerging technology
SAC provides for classification / schemes for internal control in a information system.

1. Preventive, detective and corrective.
2. Discretionary and new discretionary.
3. Voluntary and mandatory.
4. Manual and automated.
5. Application and general control.

2. COSO (Committee of Sponsoring Organization)

Define internal controls. Its components and provide criteria for internal control for management auditors staff. That is to establish a common definition an internal control and provides a standard to assess control system.
Objectives include effectiveness, efficiency of operation realizing of financial reporting and compliance with applicable laws:

- **Control environments** (Management philosophy, HR policy, operating style and integrity.
- **Risk management (**Identification and analysis of internal and external factors.)
- **Control objectives** (Policies and procedures and reviews of application and general controls)
- **Monitoring** (Special evaluation and comparison)

3. SAS (Statement of Auditing Standards)

Authoritative guide for service organization to disclose their control activities and processes to their customer and customer auditor. The user auditor should follow the guidelines of AICPA.

4. Sys Trust & Wes Trust by AI

Sys Trust was developed by IACPA & CICA, to ensure system reliability. It has four principles:

1. Availability.
2. Security.
3. Integrity.
4. Maintenance.

Web trust provide assurance for uses on website. It examine control and security issues including:

a) Privacy.
b) Security.
c) Business practices.
d) Transaction integrity.
e) Availability.
f) Confidentiality.
g) Non repetition.

6.4 IFAC Guidelines

6.4.1. Managing Security of Information

The protection of interest of those relying on information and IS and communication. That deliver the information from resulting from failure of availability, confidentiality and integrity.

Core Principles

1. Accountability.
2. Awareness.
3. Multi disciplinary.
4. Cost effective.
5. Integration.
6. IT monitoring.
7. Timeliness.
8. Social factor.

Procedure

1. Policy development.
2. Roles & responsibility.
3. Design of standard, practices and procedures.
4. Implementation.
5. Monitoring.
6. Awareness and training.

6.4.2 Managing IT practices the for business practices

IT practices should be because of its impact on business. It includes, comparison with similar organization, scheduling IS project in available resources and constrains and CBA (Cost and Benefit Analysis)

Core Principles

1. Alignment.
2. Relevant scope.
3. Relevant time frame.
4. Benefit realization.
5. Achievability.
6. Performance measurement.
7. Reassessment.
8. Awareness.
9. Accountability.
10. Commitment.

Procedures

1. Orientation
    - Set scope.
    - Establish methodology

2. Assessment of current and future needs.
    - Confirm business drivers.
    - Review technology traits.
    - Outline future environment.

- Inventory existence IS
- Assessment of what is needed.

3. Strategic Plan
    - Develop vision.
    - Desired future plan of IT
    - Option available (application, technology investment, communication, business process engineering)

4. Tactical Plan
    - Divide strategy into series of projects.
    - Set priorities based on resources.
    - Recommend monitoring and control process.

6.4.3. Acquisition of IT

Remember the following points:

1. Right solution, right times at right price.
2. No omission from business technology and legal point.
3. Importance of acquisition is directly proportioned to cost, scale and complexity.
4. Efficient use of cost and resources.
5. Progressive buy in with user involvement.
6. Valid business case.

Core principles

1. Alignment
2. Relevant requirements.
3. Obsolescence.
4. Accountability (of buyer)
5. Option analysis.
6. Evaluation.
7. Transparency.

Procedures:
It has two phases:
Phase 1: Initiate acquisition process
1. Start up and orientation.
2. Prescribing requirement (in details)
3. Evaluation criteria.
4. Contractual conditions.
5. RFP (request for proposal)

Phase 2: Solution selection (you go for selection)
1. Proposal acceptance.
2. Short listing.
3. Validity responses.
4. Conducting negotiation.
5. Solution selection.

6.4.4. Implementation of IT solution

Core principles (7)

1. Align scope.
2. Project management and commitment.
3. Managing changes, awareness and communication.
4. Selection of relevant implementation method.
5. Implementation phasing (overall phases)
6. Integration.
7. Risk management and monitoring.

Procedures (5 steps)

Phase 1: Critical design mapping
- Integration of project with existing IS
- Definition of methodology to be used.

Phase 2: Detail specification.
- Translate under requirements in to technical details.

Phase 3: Development
- Coding and customization of system
- Documentation.
- Testing.

Phase 4: Completion
- User testing.

Phase 5: Deployment
- System implemented.
- User trained.
- Final changes mode.

6.4.5 .IT SERVICES

Core principles (10)
1. Accuracy.
2. Awareness.
3. Cost Effectiveness.
4. Customer focused.
5. Disciplined approach.
6. Flexibility.
7. Meeting performance execratory.
8. Protected environment. (physical and logical security)
9. Relevance.
10. Reliability.

6.4.6 IT Monitoring

Core principles (6 steps)

1. Comprehensiveness.
2. Relevance.

3. Acceptability.
4. Reliability.
5. Action oriented.
6. Flexibility / Adaptability.

Procedure

1. Set measurable goals.
2. Verify performance.