C.A FINAL

Management Information & Control Systems

Complied By Rahul Shah ✍

PREFACE

It has been a great pleasure for presenting among the students the Summarized Notes of Management Information and Control Systems, Paper 6 in CA Final Group-II Syllabus.

The subject Management Information and Control Systems pose a great difficulty among the students community, as far as revising the whole syllabus on the last day of examination and understanding the questions in the examinations is concerned. With a view to make this task easier an endeavor has been made in these notes, to simplify and summarize the whole concept of the topic along with **in depth study in a chart format**. These notes would be immensely useful for quick overview of the subject, understanding some difficult concepts easily, quickly recapitulating the points and for the last time revision.

I feel the benefit should be passed to the student's community at large and for this reason I am presenting among you MICS Summarized notes in just 40 pages. I hope that it would also be of immense use to all of you.

Students are strongly advised to keep base as the **Institute's Study Material (M)** for detailed understanding of the subject. You can give your feedback at: shahrahul_ca@yahoo.co.in. Wishing you all the best for your future success.

Rahul Shah
Chartered Accountant

A-62, Gaganvihar,
Nr. SBI,
Khanpur, Ahmedabad – 380 001.
Ph.: 09925 450645
Email: shahrahul_ca@yahoo.co.in

Index for Contents

VARIOUS TRADITIONAL COMPUTING MODELS			
Types	**1. Main Frame Architecture**	**2. Personal Computers**	**3. File Sharing Architecture**
	• *Dumb Terminal – Intelligent Server* • *Centralised Host Based Computing Model* • *Users interact with host computer through terminals [by keystrokes]*	• *Stand Alone* • *Independent Computing Workstation*	• *Dumb Server – Intelligent Terminal* • *Server downloads entire file from shared location to desktop environment*
Importance	Allows to share computer's application, databases, peripherals	Processing load removed from central computer	GUI supported
Limitations	1. Do not support GUI & access to multiple databases from geographically dispersed sites 2. Very Costly	1. Data not shared 2. Devices like disk driver, printers, modems not shared	1. Increases response time & creates traffic in network 2. Multiple users cannot access single data concurrently

FIVE COMPONENTS OF CLIENT/SERVER ARCHITECTURE [Nov 03]				
1. Client *[Terminals]*	**2. Server**	**3. Middle Ware**	**4. Fat-Client/Fat-Server**	**5. Network**
o Client Demands o Local tasks o Front-end o Application dedicated to users	o Server Serves *[Data, service, Access]* o Global tasks o Back-end o Resources to be shared	o To allow C/S to interact o Network system implemented within C/S Tech.		o Dumb Server – Smart Workstation
Three Types Of Client	4 FDs in Web Transaction	4 Layers:**(SPOT)**	**Nov 04**	
1. **GUI** *[Windows 3.X]* 2. **Non-GUI** *[Min. Human Interaction] [ATM, Fax, Robots, Cellular]* 3. **Object Oriented User Interface (OOUI)** *[Expanded Visual Formats, Multiple Workplaces, Object Interaction][Windows 95]*	1. **File** *[Share files across network] [Maintains shared Library of Documents, Data & Images]* 2. **Database** *[Process SQL Requests from clients]* 3. **Transaction** *[Executes series of SQL Commands called OLTP; Opposite to Database Server]* 4. **Web** *[Communicate with HTTP]*	1. **S**ervice 2. Back-end/ **P**rocessing 3. Network **O**perating System 4. **T**ransport Stacks	⇒ **Fat Client** : "2 Tier Systems" *(More Processing on Client)* *Eg: File Server & Database Server* ⇒ **Fat Server** : "3 Tier Systems" *(More Processing on Server)* *Eg: Transaction, Group Ware & Web Server*	⇒ Cables, Communication Cords & Devices that link clients & Servers ⇒ Manages/ Maintains communication flow over network

RISKS ASSOCIATED WITH CLIENT/SERVER MODEL **OR** RISK INVOLVED IN TRANSITION FROM MAINFRAME COMPUTER(OR PC) TO C/S **(POET)** [Nov 02, **Nov 04**]				
Risks	1. Technological Risks	2. Operational Risks	3. Economic Risks	4. Political (People) Risks
Short-Term	o Will System Work?	o Achieve required performance from new technology?	o Cost Increase to maintain old system & new C/S development?	o Whether user & management be satisfied?
Long-Term	o Will new system work? o Will System be obsolete?	o Adapt changing needs?	o Support costs of new system?	o Costs? o Increase in cost of processing for mainframe?
To Resolve	o Understand System Standards & Market Trend	o Sound Planning & Eye to future		

KEY FACTORS FOR ACCEPTANCE OF CLIENT/SERVER TECHNOLOGY

Improvement in Direct Control & Direct Access. So, Better Service & Lower IT Cost & Flexibility
Increased data integrity & security, increased performance & better connectivity
Fast, secure, reliable, efficient, inexpensive, easy to use. Cost Reduction Technique

CHARACTERISTICS OF CLIENT/SERVER TECHNOLOGY **[MAY 03]**

Separate Process, Platform *(OS, Computer Network, Protocol)*, Upgrade;
Serve multiple clients; Networking; GUI & SQL Capability;
Application logic & Actions at client end; Data Security
Form of Distributed (shared) processing; Make use of divide & conquer logic

FOR CLIENT/SERVER SECURITY, IS AUDITOR ENSURE FOLLOWING CONTROL TECHINQUE (SEND USA) [Nov 04]

1. Disabling floppy disk drive
2. Securing automatic boot, so access becomes prohibited
3. Network Monitoring *(Helpful for later investigation)*
4. Encryption (password) technique
5. Use Smart Cards *(encryption technique to decode random code) [Temporary password]*
6. Application Controls *(Users to access only those functions required to perform their duty)*

SYSTEM DEVELOPMENT LIFE CYCLE (PARDESI) [Nov 04, **May 04, Nov 00**]

Perception & Expression OF Needs

Preliminary Investigation Stage – I Ch.-7

A. Request Clarification:
1. Defn of the Scope
2. Conducting the investigation
3. Identifying viable options

B. Feasibility (Possibility) Study: **(TELCO)**
1. Technical
2. Economical
3. Operational
4. Schedule
5. Legal

⇒ **Estimating Cost & Benefit**

COSTS :
1. Development
2. Operational
3. Intangible

BENEFITS :
1. Tangible
2. Intangible

C. Request Approval

Analysis Requirement Or System Analysis [May 02] Stage – II *(Ways Things Are)* Ch.-7

A. Fact Finding Techniques **(DIQO)**
1. Documents
2. Questionnaires
3. Interviews
4. Observations

B. Analysis of Present System

Review History, Data, Methods, Internal Controls & **Analyse** I/p, O/p, Overall & **Model** the System **[May 05]**

1. Review Historical Aspects
2. Analyse Inputs
3. Review Data Files Maintained
4. Review Methods, Procedures & Data Communications
5. Analyse Output
6. Review Internal Controls
7. Model The Existing Physical & Logical System
8. Undertake Overall Analysis

C. Analysis of Proposed System (System Analysis)

System Development Tools: [May 03, Nov 01]

1. System Components & Flows
   a. System Flow Chart (SFC)
   b. Data Flow Design/Diagram (DFD)
      i) Data Source & Destination
      ii) Data Flows
      iii) Transformation Process
      iv) Data Stores
   c. System Components Matrix
   d. CASE Tools
2. User Interface / Uses Layout Forms & Screens
3. Data Attributes & Relationship / Data Dictionary [**May 05**, Nov 02]
4. Detailed System Process

System Design *(Most Glamorous Aspect) (Like Blue Print)* **(MICS OR)** Stage – III *(Ways Things Should Be)* Ch.-8

A. Designing System Outputs
1. Output Objectives [Nov 00]
2. Imp. factors of output Design **(CONFOR²M TV)** [**May 04,** May 01, Nov 00]
   a. Content
   b. Form
   c. Volume
   d. Timeliness
   e. Media
   f. Format
3. Way of presenting info.
   a. Tabular
   b. Graphic
      - Standards in designing graphics : M 8.8
4. Design
   a. Printed O/p **[May 05]**
   b. Visual Display O/p
   c. Of Windows

B. Designing System Inputs
1. Important issues of Input Design: **(CONFORM TV)** [Nov 01, 02]
   a. Content
   b. Timeliness
   c. Media
   d. Format
   e. Volume
2. Guidelines for Form Design:
   a. Make forms easy to fill
      i) Form flow
      ii) Divide forms in logical sections
      iii) Captioning
   b. Meeting intended purpose
   c. Ensuring Accurate completion
   d. Keeping Forms attractive

C. Data Storage
   a. Conventional Files Approach
   b. Database Approach

D. Design Of Data Communication

E. System Manual *(Job Specification Manual) [Description of tasks to be performed]* [Nov 03]

F. Reporting to Mgmt.

		Consists Of 3 Activities : 1. Review System Requirements 2. Developing Model Of New System (Logical & Physical Specifications) 3. Reporting results to management

SYSTEM DEVELOPMENT LIFE CYCLE (PARDESI)

Perception & Expression OF Needs

Acquisition & Development
Stage – IV Ch.-9

Factors considered in Equipment/ Computer System Selection:
1. Latest Technology
2. Scientific vs. Business computer
3. Software supplied by manufacture
4. Compatible
5. Distⁿ betⁿ Vendor & Machine selection

Make or Buy decision of Application Software: [May 03]

Advantages Of Application Software: *[Pre written][Compared to In House]* **[Nov 04,** May 03]
1. Rapid Implementation
2. Low Risk
3. Quality
4. Cost

Sources of Acquiring Software: M 9.4 [Nov 04]

Steps involved in Selection of Computer System/ Request for Proposal: M 9.5

Criteria for Vendor Selection/Validation of Vendor's Proposal: [May 05]

Each Proposed System's:
1. Performance capability in relation to cost
2. Cost & Benefits
3. Maintainability
4. Compatibility with existing syst.
5. Vendor's support

Methods of validating proposal:
1. Checklists
   a) Software validation checklist
   b) Support service checklist
2. Point Scoring Analysis [Nov 03]
3. Public Evaluation Reports

Benchmarking Problem For Vendor's Proposal: M 9.12 [May 00]

System Testing *[To Ensure System doesn't fail]* Stage – V Ch.-9

Steps Involved:[May 01]
1. Prepare realistic test data
2. Process test data
3. Checking of results of all system test
4. Review results with future users

Program Development Life Cycle - Stages of In-House Creation of Program [May 02] **(A DESI CD² M)**
1. Program Analysis[M]
2. Program Design[M]
3. Program Coding
   3 Objectives:
   a) *Simplicity*
   b) *Efficient Utilization Of Storage*
   c) *Least Processing Time*
4. Debug the Program [May 02, Nov 01]
   a) *Use Structured Walkthroughs*
   b) *Test the Program*
   c) *Review the Program code for adherence to standards*
5. Program Documentation
6. Program Maintenance [M]

M = Managers are involved

Implementation & Maintenance *[Continuous Iterative Process]*
Stage – VI Ch.-10

4 Major Aspects Of Implementation: (CEPT)
1. Equipment Installation
   a) Site Preparation
   b) Equip. Installation
   c) Equip. Checkout *[Extensive tests]*
2. Training Personnel (Trouble Shooting) **[May 03]**
   a) System Operators (Professionals/Data Entry Personnel)
   b) Users
3. Conversion Procedure
   Activities for successful conversion (PASS Fail) [May 05]
   a) Procedure Conversion
   b) File Conversion
   c) System Conversion
   d) Scheduling Personnel & Equipment
   e) Alternative Plans in case of equipment failure

   5 Strategies/Methods for conversion (Manual to computerized) (PGD²M) [May 00] [Nov 03]
   a) Direct Changeover
   b) Parallel Conversion
   c) Gradual Conversion
   d) Modular Prototype Conversion
   e) Distributed Conversion
4. Post-Implementation Evaluation (Feedback) **[Nov 04]**
   a) Development Evaluation
   b) Operation Evaluation
   c) Information Evaluation

   2 Basic Dimensions evaluated:
   a) Syst. Operating Properly
   b) User is satisfied

Program Design Tools:(4 PSPO) [May 04] 1. Program Flow Chart 2. Pseudo Code 3. Structure Chart 4. 4thGL Tools 5. Object Oriented Programming & Design Tools		**Maintenance in 2 ways :** [May 01, Nov 02] 1. Scheduled Maintenance 2. Rescue maintenance

Stage – I : Preliminary Investigation

A. Request Clarification: [What originator wants]

1. Defn of the Scope *(Shifting Business Requirements, Changing Organization Environments, Evolving Info. Technology, Proposal Submitted to Steering Committee)*
2. Conducting the investigation
   Analysts collects data by:
   a. Reviewing Internal Documents *(organization charts) (Operating Procedures)*
   b. Conducting Interviews *(of Mgmt. & Supervisory Personnel)*
3. Identifying viable options (Numerous Possibilities)
   Key Ingredients : Common Sense & Intuition

B. Feasibility (Possibility) Study: (TELCO)-{Evaluating alternative Systems through Costs/Benefits Analysis}

1. Technical *[Hardware, Software] [Technical Guarantees Of Accuracy, Reliability & Ease of Access, Data Security] [Technical capacity to hold data, System expanded if developed]* – M 7.19
2. Economical *[Evaluation of incremental cost & benefits expected] [Most difficult aspect of Study]*
3. Operational *[Finding reviews of workers, employees, customers & suppliers about use of computer facility]*
   [Support or lack of support by employees is critical aspect]
4. Schedule *[Design Team Estimation]*
   [Time to take new/revised system to became operational]
5. Legal *[Comply financial Reporting requirements & Co.'s contractual obligation]*

⇒ Estimating Cost & Benefit

COSTS :

1. Development *[Cost of testing, documenting training, start up costs, salary of program designers, preparing & converting data files]*
2. Operational *[Salary of computer operators, system analysts maintaining system, cost of input data, cost of maintenance, overhead charges, rental/depreciation charges]*
3. Intangible (Indefinable) *(Goodwill lost by error during installation of new system) [Loss to employee productivity, self confidence]*

BENEFITS :

1. Tangible *[Accurately measured]*
   - *Increase in sales/profits, operational ability, efficiency*
   - *Decrease in data processing cost, operating cost, investment*
   - *Improved info. availability, computation & analysis, customer service, employee morale, mgmt. decision, competitive position, business image*
2. Intangible *[Improved business image] [Hard to measure & define]*

C. Request Approval: *[Based on observation of analyst]*

Stage – II : Analysis Requirement Or System Analysis

[Study in depth present & proposed system]

A. Fact Finding Techniques (DIQO)

1. Documents *[Bill, manuals, diagrams, forms] [Organization charts] [current, accurate, up-to-date]*
2. Questionnaires *[In traditional approach only] [Skillfully Drafted]*
3. Interviews *[Personal contact, Body language]*
4. Observations *[In Prototype] [When not aware, surprise visit]*

***Review** History, Data, Methods, Internal Controls & **Analyse** I/p, O/p, Overall & **Model** the System.*

B. Analysis of Present System

[To identify problems & Shortcomings]

1. Review Historical Aspects *[Logical starting point, Identify major turning points & milestones that influenced it growth]]*
2. Analyze Inputs *[Imp. as basic to manipulation of data]*
3. Review Data Files Maintained *[All online/offline files]*
4. Review Methods, Procedures & Data Communications *[Eliminate unnecessary tasks]*
5. Analyze Output *[What information, Why, Who, When, Where?]*
6. Review Internal Controls *[Locating control points]*
7. Model The Existing Physical *[DFD-Detailed]* & Logical System *[SFC-Overview]*
8. Undertake Overall Analysis

C. Analysis of Proposed System

(System Analysis) *[To Steering Committee] [Consideration to strength & weaknesses of present system] [OUTPUT-to-INPUT process]*

System Development Tools: *[To improve current IS & develop new ones]*

1. System Components & Flows *[Overview of system & Flow of data]*
   a) System Flow Chart (Logical) *[Used to communicate overall structure & flow to end user] [Graphic model of physical info. System exist/proposed] [Shows Hardware devices & Manual activities]*
   b) Data Flow Design/Diagram (Physical) *[Used by analyst to gather information; Flow of data within org^n] [No ideal way to develop DFD] [Subdividing of DFD-Highest Level DFD is Context Diagram provides summary level info]*
      i) Data Source & Destination (Sinks) *[People & organization sends/receives data to/from system]*
      ii) Data Flows *[Can consists of One or more pieces of datum]*
      iii) Transformation Process *[Bubbles] [Transform data from i/p to o/p]*
      iv) Data Stores *[Temporary/Permanent repository (store house)]*
   c) System Components Matrix *[Required process by required people] [Matrix framework documents resource used, activities performed & information produced by IS] [Highlights how i/p, processing, o/p, storage & controls are accomplished]*
   d) CASE Tools *[Software packages offering onscreen drawing modules] [Generates DFD & SFC] [Automation]*
2. User Interface *(Uses Layout Forms & Screens, Use 4GL, CASE Tools) [Designing interface between users & computer] [Ans like 'Y' 'No' 'Cancel']*
3. Data Attributes & Relationship *(Data Dictionary)*
4. Detailed System Process *[If above not helpful] [Decision Tree/Table, Structure Charts]*

DATA DICTIONARY *[Computer file about data]*

Uses:	**Data Dictionary Contains:**
1. Aids in documentation *[To Programmers & analysts]*	1. Data item's length, type & range
2. File Security	2. Identity of source document used to create data item
3. For accountant *(Planning flow of transaction data)* and auditors *(establish audit trail)*	3. Names of computer file storing data item
4. Aids in investigating / documenting internal control procedures	4. Names of computer program that modify data item
	5. Identity of individual permitted to access
	6. Identity of individual not permitted to access

VARIOUS APPROACHES TO SYSTEM DEVELOPMENT **(PETS TB)**

<table>
<tr><th>1. Traditional Approach</th><th>2. Prototyping Approach [May 00, Nov 02]</th><th>3. End User Development Approach</th><th>4. Top-Down Approach</th><th>5. Bottom-Up Approach</th><th>6. Systematic Approach For Development</th></tr>
<tr><td>1. Activities perform in sequence
2. Management/user review the work & sign-off
3. Next activity is undertaken only when the prior step is fully completed</td><td>1. Develop Small or Pilot Version
2. <u>Four Steps:</u> [May 04]
a) Identify Info. System requirements (Less formal & less time consuming)
b) Develop Initial Prototype (Rapid Development & Low Cost) (Simplicity, Flexibility & Ease Of Use)
c) Test & Revise (User Feedback, Iterative process of modification & re-evaluation)
d) Take user sign-off (Establish Contractual Obligation & Develop Fully functional Systems)</td><td>1. No Professionals, Low cost technology
2. Risks:
Reduction in:
a) Standards & Control
b) Accuracy
c) Quality & Assurance
d) Stability
e) Compatibility
f) Access to Corporate Database (Central System)</td><td colspan="2">Difference [Nov 99]</td><td>⇒<u>In Small Organisation</u>
<u>Stages Involved:</u>
1. Identify Requirements
2. Locate, evaluate & secure suitable software
3. Locate, evaluate & select suitable hardware for software
4. Implement the system

⇒To develop Office Info. System in own work areas</td></tr>
<tr><td>⇒Best Suited For:
CBIS, as processing requirements are best understood
Eg: TPS</td><td>⇒Ideal For:
1. DSS [Experimentation and Trial & Error Development]
2. ES and MIS
3. During System Design Stage to develop fake screen for output</td><td>⇒Best Suited For: Single Manager & Single Department</td><td>1. Secularism (Worldly Matters)
2. Top Mgmt. formulates major objective, strategies & policies
3. Info. System development is more consistent with systems approach
4. High degree of Top Mgmt. Involvement</td><td>1. Democracy (By-The-People)
2. Supervisory Mgmt. Identifies the life stream systems
3. Info. System is developed through an orderly process (of transition)
4. Syst. Development done by supervisory level</td><td></td></tr>
</table>

VARIOUS APPROACHES TO SYSTEM DEVELOPMENT (…….contd.)

1. Traditional Approach	2. Prototyping Approach	4. Top-Down Approach	5. Bottom-Up Approach *[Life stream/ day to day activities]*
⇒Managers review diagram / explanation charts to ensure accurate/complete work ⇒During Pre. Invest. & Req. Analysis, Syst. Development activities are led by system analysts ⇒During later stages, they turn over project to system designers	**Advantages :** 1. Users are involved *(Make suggestions & improvement)* 2. Short Term Period & less costly *(System Built Quickly)* 3. Less error prone 4. Clear visual picture of final version 5. Signals impractical situation & saves time & money **Disadvantages:** 1. Many experiments 2. Time Devotion *(By Syst. Users & provide syst. Developers with suggestions)* 3. High Risk associated with developing & implementing wrong system 4. Not appropriate for designing large/complex info. systems where I/p, Process & O/p are clearly defined 5. Not used for Traditional AIS Application ⇒Inadequate Testing make system error-prone ⇒Inadequate Documentation make system difficult to maintain	**Stages:** 1. Analyze Objectives & Goals of organization 2. Identify function of organization & explain how they support entire organization 3. Ascertain major activities of managers 4. Identify models that guide managerial decision process --- o *What info. Needed?* o *When needed?* o *In Which Form?*	**Stages:** 1. Identifying the basic transactions, info. file requirements & info. processing programs 2. Integration of data of each info. system *[enhances shareability & evolveability of database]* 3. Addition of decision models & various planning models to support higher mgmt. activities 4. To formulate alternative strategies

CATEGORIES OF INFORMATION SYSTEMS [Nov 01]

Transaction Processing System (TPS)	Management Info. System (MIS)	Decision Support System (DSS)	Executive Info. System (EIS) [Nov 03]	Expert System (ES) [May 04]
o Recurring, Structured, Routine Problems o Operations Oriented o Ensure capture of appropriate data & accurate info. reporting o Provides framework for analyzing an organization's activities & o Also offer systematic framework for analysis & design of AIS	o Use results produced by TPS o Structured, Repetitive, Predictable Problems o Decision Making, Problem Solving o Info. critical for success of bus. org^{n}. o Network of info. supports Mgmt. DM o Possess characteristics of MRS-Provides fixed preformatted info. in standardized way	o Moe flexible & adoptable to changing DM requirements than traditional MRS o Semi-structured/ Unstructured Decision, Unique (Non-recurring) o Alternatives for making decision o Supports for taking decision at Tactical Level & Strategic Level could make best use of it o Greater flexibility o Not seen as standalone system but as an integrated piece of software o Supports human DM rather providing means to replace it o Eg: Sensitivity Analysis, Spread Sheet	o Finalization by Top Mgmt. o Strategic Problems o Model Complex Problems o Easy to Use, Graphically based o Uses external & internal data	o Final Solution for Decision o Real Expert, Give Judgment o In specific area & not general o Arisen from academic research into artificial intelligence o Replaced subjective DM

System Design (Stage III)

A. Designing System Outputs (O/p)

a. Output Objectives
1. Convey info about past, current, future
2. Signal Imp. Events *[Alarm, Timer]*
3. Trigger an action
4. Confirmation of action *[Yes/No]*
5. Meets needs of organisation & users

b. Imp. Factors of Output Design **(ConFor²M TV)**
1. **Con**tent *(Actual pieces of data) [Only required info.]*
2. **For**m *(Way in which content is presented to users) [Summary & Detailed] [Text, Graphics, Video, %]*
3. **V**olume *(Printer, High Speed rapid retrieval display unit) [Too high volume → More paper cost → COM] [O/p at any one time]*
4. **T**imeliness *(When user need o/p) [Real time system]*
5. **M**edia *(Physical Device for i/p, storage , o/p) [Paper, CD, Voice o/p]*
6. **For**mat *(Data physically arranged)[On Printed report or Display Screen; Print Preview]*
   - Real issue is not how much can be provided but it is how little needed to make imp. info. available

c. Way of presenting info.
1. Tabular *[Details dominate & few explainations needed]*
2. Graphic *[Enhances mgmt. presentation & improves effectiveness of o/p reporting] [Pie, bar, area Charts, Maps]*

d. Design / Layout form of
1. Printed O/p
2. Visual Display O/p
3. Of Windows
   i) Order inquiries
   ii) A/cs payable verification

C. Data Storage

1. Conventional Files Approach *(In traditional system where each transaction is updated to record in master file)*
2. Database Approach *(Support mgmt. decision making & same data in multiple application)*

B. Designing System Inputs (I/p)

Important issues of Input Design: (ConForM TV)
1. **Con**tent *[Data for required o/p]*
2. **T**imeliness *[Imp in TPS as i/p person & o/p person are different]*
3. **M**edia *[Keyboard, OCR, voice I/p, MT, MD]*
4. **For**mat *[Type & length of data field]*
5. **V**olume *[Amt. of data entered at any one time]*

Guidelines for Form Design:
1. Make forms easy to fill
   a) Form flow *[Min. time & effort] [→ ↓]*
   b) Divide forms in logical sections *[7 Pts.]*
   c) Captioning *[Title heading]*
2. Meeting intended purpose *[Recording, processing, storing, retrieving info.]*
3. Ensuring Accurate completion *[Various controls – Row & Column Totals] [Error rate drops]*
4. Keeping Forms attractive (aesthetic–*Different fonts*) *[Neat, organized & logical; Proper layout & flow]*

CODING METHODS: To reduce input control errors & speed up entire process

Characteristics Of a Good Coding Schemes or Coding Methods: [May 05, Nov 01] **(SPICES)**
1. **I**ndividuality *[Unique, universal]*
2. **S**pace *[Brief]*
3. **C**onvenience *[Short & Simple; Avoid special symbols]*
4. **E**xpandability *[Future growth possible]*
5. **S**uggestiveness *[Not too lengthy] [Understandable]*
6. **P**ermanence *[Not invalidate]*

Coding Schemes: (FM HSC) [Nov 01]
1. **C**lassification codes *[Simplify i/p process as only single digit required] [different classes of events, people, object]*
2. **F**unction Codes *[State activities to be performed without spelling out all details]*
3. **S**ignificant digit subset codes
4. **M**nemonic codes [MBA] *[Symbolic] [Suitable when to be remembered]*
5. **H**ierarchical classification *[Progressive codes] [Used in almost any business]*

Logical Design	Physical Design
o System design first involves logical design o Write detailed specification of new system called design specification o Like engineering blue print showing major features & how they are related	o It is an activity following logical design o Produces program software, files & a working system o Design specification instructs programmers what system should do

Stage – IV : System Acquisition & Development Stages

Factors considered in Equipment Selection / Procuring Computer Hardware:

1. Latest Technology *[Better Performance & Low Cost]*
2. Scientific vs. Business computer *[Speed, Storage, Computational facilities]*
3. Software supplied by manufacturer *[General & Special]*
4. Compatible *[Upgradation]*
5. Distⁿ betⁿ Vendor & Machine selection *[Configuration & Plan for Gradual expansion] [Business Judgement]*

Advantages Of Application Software *[Pre written]***: [Compared to In House]**

1. Rapid Implementation *[Readily Available]*
2. Low Risk *[of Quality & Cost] [Available in finished form]*
3. Quality *[Tried & Tested]*
4. Cost *[No Hidden Cost] [Vendors can leverage development cost]*

Criteria for Vendor Selection / Validation of Vendors Proposal:

Each Proposed System's

1. Performance capability in relation to cost *[Use Benchmark Test]*
2. Cost & Benefits *[Purchase or Lease]*
3. Maintainability *[Modification] [Place considerable emphasis]*
4. Compatibility with existing system *[Ability to implement & interface – both hardware & software issues]*
5. Vendor's support *[Training, Implementing, Testing, Maintaining backup] [Business Hours Vs. Round The Clock]*

Methods of validating proposal:

1. Checklists *[Criteria in form of ques.][Most Simple Method]*
   a. Software validation checklist
   b. Support service checklist
2. Point Scoring Analysis
3. Public Evaluation Reports *[When buying Staff has inadequate knowledge]*

Two Questions Remain:

1. Are Present Users Satisfied & Vendor's Support?
2. Will System Perform as vendor claims?

Program Design Tools: (4PSPO)

1. Program Flow Chart *[Logical processing steps; Do not provide broad view] [Mathematical/Scientific Problem]*
2. Pseudo Code *[Eng. Like statements, user friendly] [Designing TPS & Info. retrieval program]]*
3. Structure Chart *[Like orgⁿ charts] [Organizes each program task into well defined modules]*
4. 4thGL Tools *[Automation & consistency leads to productivity gains]*
5. Object Oriented Programming & Design Tools *[Enhancing productivity & reducing time] [Taken from DFD]*

Stage – V : System Testing *[To Ensure System doesn't fail]*

Steps Involved:

1. Prepare realistic test data
2. Process test data
3. Checking results of all system test
4. Review results with future users, operators & support personnel
   - Most effective way of system level testing – Perform Parallel Operations

Program Development Life Cycle - Stages of In-House Creation of Program **(A Desi CD² M)**

1. ᴹProgram Analysis *[Whether proposed application be programmed?] [Programmer Studies available Input, Processing & Output]*
2. ᴹProgram Design *[Develops general layout of program] [Input, Output, File Layouts & Flow Chart are useful tools]*
3. Program Coding *[Convert logic into Programming Language] [By interpreter or compiler (I/C)] [Coded instruction (entered in →) Magnetic Media – consists source program (written in assembly/higher level language-Basic/C) (translated by I/C into →) Machine language*

   3 Objectives:

   a) Simplicity
   b) Efficient Utilization Of Storage
   c) Least Processing Time
4. Debug the Program *[Tedious Task] [Correcting Programming Language Syntax & Diagnostic errors, so, program **'Compiles Cleanly'**] [By Batch (Few Days) / Interactive (Few Hours) Compiler] [Testing Procedures to make program error free] [DEBUG :- ❶ Source Program into Compiler ❷ Finds error ❸ Corrects error ❹ Resubmit to compiler after correction]*
   a) Use Structured Walkthroughs *[Mental execution of program; Examine Source Text]*
   b) Test the Program *[Essential for successful installation; Keep log of test results]*
   c) Review the Program code for adherence to standards
5. Program Documentation *[User Manual] [Ensure software/system behaves as documentation indicates] [User can clearly understand & not in computer terminology]*
6. ᴹProgram Maintenance

M = Managers are involved

4 Major Aspects Of Implementation (CEPT)			
1. **E**quipment Installation	2. **T**raining Personnel	3. **C**onversion Procedure	4. **P**ost-Implementation Evaluation (Feedback)
1. Site Preparation *(To Be completed prior to delivery of equipment; Operation Environment; Space Layout)* 2. Equipment Installation 3. Equipment Checkout *(Run Extensive test of own by user)*	1. System Operators (Professionals / Data Entry Personnel) *(Trouble Shooting & Remedies; Routine & extraordinary)* 2. Users (Operators) *(Data handling activities)* o Training deficiencies can translate into reduced user productivity levels	**Activities for successful conversion (PASS Fail)** 1. **P**rocedure Conversion *(Operating procedure documentation) [Open communication]* 2. **F**ile Conversion *(Online/ offline files) [Thorough test & adequate control]* 3. **S**ystem Conversion *(Cut Off dates)* 4. **S**cheduling Personnel & Equipment *(Daily/Monthly Schedule) [Realistic] [Interactive System : Difficult as not predictable & Batch Processing System : Predefined]* 5. **A**lternative Plans in case of equipment failure *(Responsibility of Computer Section) (Priority to critical jobs)* **5 Strategies/Methods for conversion/changeover of old system to new system (Manual to computerized) (PGD²M)** a) **D**irect Changeover b) **P**arallel Conversion *(Old & New System Simultaneously)* c) **G**radual Conversion *[Best Features Of a) & b)]* d) **M**odular Prototype Conversion *(In parts)* e) **D**istributed Conversion	1. Development Evaluation *(Developed on schedule & within budget)* 2. Operation Evaluation *(Whether Hardware, Software, Personnel capable of performing duties) (Quick Response time) [Evaluation criteria established in advance]* 3. Information Evaluation *[Difficult & cannot be conducted in quantitative manner] (User satisfaction by Interview & Questionnaire Technique)* **2 Basic Dimensions :** a) Syst. Operating Properly b) User is satisfied

5 Strategies for Converting Old System to NewSystem [Manual to Computerised]

Adequate Planning, Scheduling, Security important for successful changeover **(PGD²M)**

Strategies	1. **D**irect Changeover	2. **P**arallel Conversion	3. **G**radual Conversion	4. **M**odular Prototype Conversion	5. **D**istributed Conversion
	○ *Old System is dropped & new system put to use* ○ *Extensive training in advance*	○ *Old & New System Simultaneously* ○ *After some time old one is stopped*	○ *Best Features of 1. & 2. without risk*	○ *In parts - Gradual Manner*	○ *Installation of same system at different sites [with any 4 approaches]*
Advantages	1. No possibility of using old system 2. Adaptation	1. Checking accuracy of new with old 2. Feeling of security to users as not forced to change 3. Best for manual to computerized	1. Allows users involve with system gradually 2. Detecting & recovering errors without lot of downtime	1. Each module thoroughly tested 2. Familiarity	1. Problems detected and controlled in succession
Disadvantages	1. Long delays if error occur 2. Users dislike to unfamiliar System without alternative 3. Comparison of old/new system difficult 4. Risky approach to conversion	1. Cost 2. Workload during conversion *(doubled)* 3. Comparison difficult if system replaced is not a manual one 4. Employees faced with choice continue using old system	1. Too long to replace new system 2. Inappropriate for conversion of small/uncomplicated system	1. Prototype not feasible 2. Special attention to interfaces, as whether modules built does actually work	1. Each site have its own peculiarities to work

Maintenance Can Be In 2 Ways

1. Scheduled Maintenance *(Annual Maintenance Contract) [Pre planned]*
2. Rescue Maintenance *(Virus Scanning software) [Change due to undetected error-malfunction]*

Enterprise Resource Planning

- **Evolution:** [May 03] Need for standard software package, to gain competitive edge in volatile business environment, which can integrate & synchronize the isolated function into streamlined business process.
  - In volatile business environment, it is impossible to create & maintain custom-designed software package which cater all requirements & be up-to-date.
  - MIS → IIS [Integrated] EIS [Executive] CIS [Corporate] EWS [Enterprise Wide Systems] MRP [Material (MPS/BOM)] MRP II [Manufacturing to ERP evolution] MRP III [Money]
- **Meaning:** ERP software is fully integrated business management system & latest high-end solution provided by IT to business applications.
  - Synergize MEN, MATERIAL, MONEY & MACHINE.
  - Promises one database, one application, one user interface for entire enterprise *[Single integrated software]*
  - Assists employees & managers to plan, monitor & control entire business.
  - Whole being greater than sum in parts.
  - Integrated info. storehouse wherein info. is stored at one place.
  - ERP is not a single system but a framework that includes Administration Application *[Fin, A/cing]*, HR Application *[Payroll, Benefits]* & Manufacturing Resource Planning Application *[Procurement, Production, Planning]*. It unites major business processes into single family of software modules.
- **Pre-requisite:** Sophisticated IT infrastructure for Co. having multiple location of operation & control, facilitating Online Data Transfer.
- Business Modeling is basis by which one can select & implement suitable ERP Package.
- **Characteristics: [May 05]**
  1. Flexibility *[Respond to changing needs & C/S Technology enables to run across various database back ends through ODBC]*
  2. Modular & Open *[Connect or detach any module]*
  3. Comprehensive *[Wide Ranging]*
  4. Beyond the Co. *[Support online connectivity to other entities]*
  5. Best Business Practices *[Collections]*
- **Features: [May 05]**
  1. MULTI-FACETED: Provides Multi-Platform, Multi-Facility, Multi-Mode manufacturing, Multi-Currency, Multi-Lingual facilities
  2. Supports strategic & business planning, Operational planning & execution activities, Creation of materials & resources.
  3. Performs core activities & increase customer service, thereby increasing corporate image.
  4. Bridges info. gap.
  5. Allows automatic introduction of latest tech. like EFT, EDI, Internet, Video conferencing, E-Commerce, etc.
  6. Eliminates most business problems.
  7. Provides intelligent tools like DSS, EIS, Data Mining.
  8. Better Project Management.
- **Benefits** *[Unlimited]*: M. 12.6

Business Process Re-engineering (BPR) [Nov 04]

- **Meaning:** Fundamental Rethinking *[Asking "Why do you do what you do" i.e. eliminating process not adding value to customers]* and Radical Redesign *[Says "whatever you were doing in past was all wrong"; Reinventing & not enhancing/improving]* of process to Achieve Dramatic Improvement *[By major transformation 80 to 90% reduction and not 5 to 10%]* in cost, quality, service & speed.
- May or may not require IT.
- Every Co. intending to implement ERP has to re-engineer its process in one form or another known as BPR.
- BPR is the pre-requisite for going ahead with a powerful planning tool like ERP.

Business Engineering (BE)

- **Meaning:** Rethinking of business processes to improve, speed, quality & output of materials/services.
  - Process oriented business solutions enhanced by C/S computing in IT.
  - BE comes out of merging IT & BPR.
- Main point of BE is efficient redesigning of Co.'s Value Added Chains *[Series of connected steps running through business]*
- Method of development of business processes according to changing requirements.
- Business Management = Virtual Corporation + ERP Software

Business Modeling

- **Meaning:** Diagrammatic representation of business as one large system with inter connections of business systems it comprises of.
- 1st Step of ERP implementation is developing business process model using MIS Planning.
- Planning to arrive at process is done Top Down whereas MIS implementation is from Bottom up.
- Data Model consists of two elements:
  1. Diagram describing various business process & their interactions.
  2. Underlying (Basic) Data Model.
- Helps to check how well model fits into application.
- SAP, a popular ERP package uses Event Driven Process Chain (EPC) methodology to model business process.

Steps in ERP Implementation / ERP Implementation Methodology

1. Identification of needs
2. "As Is" Analysis *[SWOT Understanding]*
3. "Would Be" Estimation *[Benchmarking (in cost, quality, service]*
4. BPR
5. ERP Package Evaluation *[Features of ERP]*
6. Finalizing the Package *[Comparison of critical factors through Matrix Analysis]*
7. Equipment Installation *[Phased Manner]*
8. Appointment of Consultants *[Skill, Experience, Cost]*
9. Implementation

- General Implementation Guidelines for ERP : M.12.16 [Nov 03]

Expectations & Fears at the beginning of Post-Implementation and Realities Organization must keep in mind [Nov 04]

- **Expectations:**
  1. Improvement in processes
  2. Increased productivity
  3. Total automation & ending of all manual processes
  4. Improvement of all KPIs
  5. Elimination of all manual record keeping
  6. Real-Time IS available on need basis
  7. Total integration of all operations
- **Massive Fears:**
  1. Job redundancy(security)
  2. Lack of importance
  3. Change in job profile
  4. Loss of proper control & authorization
  5. Increased stress by greater transparency
  6. Loss of authority
- **Realities Organization must keep in mind:**
  1. Changing involves 3 levels:
     a) Strategic
     b) Business Process & Change
     c) Consequential Organization change
  2. Willingness to change (attitude)
  3. Measuring KPIs
  4. Process peculiar to some sectors (to be done manually)
  5. Implementation is not end of the road and continuous improvements is required to reap benefits

Life of an ERP after implementation

- Main tool – Process of communication *[written, oral, workshops, meetings]* in all forms
- Educating all layers of management in – functionality, limitations & benefits
- CSFs of whole co. should be listed
- From CSFs, required performance measure should be called out
- NUMERIC FIGURES against these performance measures is called KPIs *[Done through workshops]*
- This process to be completed before ERP Configuration
- Imp. End users should be involved in process
- Tasks to be performed to suit future ERP environment:
  - Develop new job description & organization structure to suit post ERP Scenario
  - Determine Skill gap between existing & envisioned jobs
  - Assess training requirement & create & implement training plan
  - Develop & amend HR, Financial & Operational policies
  - Plan for workforce logistics adjustment

Problems while performing Post-Implementation / Post Implementation Blues

- Major task is to monitor the KPIs & take correct business decision to improve them
  - Set attainable goals & stretched target in phases
- Legacy (in heritage) systems run for period of time only for data transfer or just to be safe. Users display resistance to change
- EDP Audit: General or specific to evaluate security, authorization & controls. Need for course correction due to
  - Change in business environment causes change in CSFs KPIs which necessitate reconfiguration
  - Need for change in some process
  - Vision change in ERP & improvement in hardware & communication technology
  - New addition require extra functionality
- International trend is to outsource maintenance & up gradation to enable to concentrate on core activity

ERP Software Package (SAP)

1. Financials *[Financial Accounting, General Ledger, Accounts receivable and payable, Fixed asset accounting]*
2. Controlling *[Overhead Cost Control, Cost centre accounting, Overhead orders, Activity Based Costing, Product cost control, cost object controlling, Profitability analysis]*
3. Investment Management *[Corporate wide budgeting, Appropriation requests, Investment measures, Automatic settlement to fixed assets, Depreciation forecast]*
4. Treasure *[Cash Management, Treasure Management, Market risk Management, Funds Management]*
5. Integrated Enterprise Management
6. Product Data Management
7. Sales & Distribution
8. Production Planning & Control
9. Materials Management *[Purchasing, Inventory Management, Warehouse Management, Invoice Verification, Quality Management, Plant Management, Service Management]*
10. HR Management *[Personnel administration, Employee master data, Recruitment Management, Open positions, Selection and hiring, Travel Management, Benefits Administration, Personnel cost planning]*
11. Pay Roll Accounting *[Payroll processing, Integration, Global solutions, Time management, Time data, Time evaluation, Time Management review, Integration and Interfaces, Shift planning]*
12. Internet & Intranet

Reasons for EDP System Controls

1. Process more data. So, greater potential errors.
2. Human supervision of data accuracy & integrity not possible as process & store data in **non-human readable.**
3. Blurred (unclear) audit trail.

General Controls In a Computer Based System

1. Operation system controls
2. Data Management controls
3. Organizational structure controls
4. Systems Development controls
5. Systems Maintenance controls
6. Computer centre security controls *[Physical Security]*
7. Internet & Intranet controls
8. Personal computer controls

Controls in Computer Based System

General controls apply to a wide range of exposures that systematically threaten the integrity of all application processed within the CBIS environment.

Application controls are focused on exposures associated with specific systems such as payroll, accounts receivables, etc.

1. Operating System Controls *(System responsible for Operating Computer)* [Transportation vehicle bet^{n} User & Hardware]

3 Main Tasks [Allows users & their applications to share & access common resources]	**5 Control Objectives** [2 Perform tasks Consistently & Reliably]	**Security Components** [Who *Access*, Which *Resources*, What *Actions*]	**Threats To System Integrity** [Reliability]	**Controlling Against:**		**Audit Trail Objectives** [Imp. Detective Control] [Logs to record activity at system, application & user level]
1. Translates high level languages into machine level language 2. Allocates computer resources to users, workgroups & applications. 3. Manages job scheduling & multiprogramming.	Protect: 1. Itself from Users *[Application]* 2. Users from each other *[Storage Partition]* 3. Users from themselves *[Module]* 4. From Itself *[Module]* 5. From Environment *[Humidity, Power Failure] [Scan Disk after re-start]*	1. Log-on Procedure *[User-ID & Password] [1st line defense]* 2. Access Token *[To approve all actions by user] [contains user's key info.]* 3. Access Control List *[Like Data Auth. Table] [Matches rights granted to users; Controls access to system resources]* 4. Discretionary (Optional) Access Control *[For Specific resources] [Closely supervised to prevent security break]*	1. Accidental *[Unintentional disclosure of confidential info.] [Hardware Failure, Error in user application program]* 2. Intentional a. *Privileged personnel abuse authority* b. *Identify & exploit security flaws* c. *Insert computer virus / Destructive Program*	**(A) Access Privilege/ Rights** Passwords *(System, Application, Files, Network)*: 1. One-Time *[Secret Reusable PIN + One Time Password]* 2. Reusable *[Use Smart Password & not weak]*	**(B) Viruses/ Destructive Programs** 1. Virus 2. WORM 3. Back Door / Trap Door 4. Logic Bomb 5. Trojan Horse	1. Detect Unauthorised Access *[Real time detection or After the fact]* 2. Reconstruct events *[Audit analysis] [Knowledge of conditions at time of failure]* 3. Personal Accountability *[Preventive Control] [Monitor user activity at lowest level]* 4. Implement an Audit Trail *[Measuring potential damage & Financial loss] [Assessing adequacies & need of additional control]*

2. Data Management Controls

1. Access Control [May 05] *[Not necessary in Flat File System (cannot share) i.e. necessary in shared database] [Prevent unauthorised users from viewing, retrieving, corrupting, destroying entity's data]*

1. User View *[Sub schema] [What user wants, Logical View] [Do not define authorisation rights]*
2. Data Authorisation Table *[Like Access Control List] [Rules to limit actions users take]*
3. User Defined Procedure *[Series of personal questions]*
4. Data Encryption (Coding) *[Password]*
5. Bio-Metric Devices *[Thumb print, Eye Retina, sign.] [Currently used to secure ATM cards]*

2. Back-up *[Copy of Current file for security]* **Control** *[In the event of data loss org^n can recover its files & databases] [Originals stored at physically distant site]*

A. File Security
[For reconstruction of files on:]

Magnetic Disk / Hard Disk Failure

Contents of Master file is periodically copied on Magnetic Disc/Tape Backup File & stored at another location. It Serves 2 Purposes :

1. *As transactions occurs constantly, provides links from one backup file to another*
2. *Providing records that caused change, as writing on Magnetic Disk is by Overlaying Technique.*

Magnetic Tape

G-F-S *[Generation Technique]*
[Files relating to two previous periods are retained in addition to current updated master file & current transaction file]

B. Back-up Control in Database Environment [DBMS]

1. Back up of Database *[In secure remote area]*
2. Transaction Log *[For Audit Trail] [Records changes to database]*
3. Check Point *[Auto Saving] [For Reconciliation of transaction log & database change log against database] [If failure – restart from last check point]*
4. Recovery Module *[To Restart after failure]*

3. Organisation Structure Controls [Separating/Segregating functions Of]

In manual environment, following operational tasks are segregated:

1. Transaction authorization from transaction processing.
2. Record keeping from asset custody.
3. Divide transaction processing task, so perpetration of fraud requires collusion.

- In CBIS, transaction processing tasks are performed by computer programmers so focus of control shifts from operational level to higher level.

Segregating System Development From
Divided into : System Analysis *(design new system)* & Programming group *(codes program according to design specifications)*

Database Administrator *[As DBA is responsible for critical tasks pertaining to database security like creating database schema, user sub schema, assigning access authority, monitoring & planning for future expansion]* **from other function** *[Organizationally Independent]*

Maintenance *[Problems due to combining Application Programming (By programming group) & Maintenance]*

1. Inadequate Documentation
   a) Not as interesting as designing, testing & implementing
   b) Job Security *[Gives power & becomes indispensable (essential)]*
2. Program Fraud

Computer Operations
[Segregating Development from Operations – Greatest Important]
[Relation is extremely formal & they only run systems and have no involvement in system design]

Give an alternative structure for System Development

1. *Improve Documentation Standards [May use CASE tools]*
2. *Denying original programmer future access*

From Data Library
[For physical security of off-line data files]

- *Controlled access by Data Librarian*
- *Keep detailed log*
- *Expiration dates*

4. System Development Controls **[May 04]**

1. System Authorisation *[Formal, Properly Authorised, Written request by user to system professionals]*
2. User Specification *[User involvement should not be ignored b'coz of high degree of technical complexity]*
3. Technical Design *[Analysis & Design] [Quality of documentation critical for system long term success] [Documentation is control & evidence of control]*
4. Internal AuditParticipation *[Plays imp. role in control] [Involves auditor in entire SDLC for conceptual suggestions]*
5. Program Testing *[Testing before implementing] [Test result against Pre determined result to identify programming & logic errors] [Time consuming]*
6. User Test & Acceptance *[Test team should be satisfied that system meets its stated objectives]*

5. System Maintenance controls **[File control: May 00]**

1. Maintenance, Authorisation, Testing & Documentation –
   - All maintenance action requires minimum 4 controls: (1) Formal Authorisations (2) Technical Specifications (3) Testing (4) Documentation Updates.
   - Essentially same treatment as new development. Extent of change & its potential impact, govern degree of control applied *[More change, More control]*
2. Source Program Library (SPL) Control –
   - Application Program Modules are stored in Source Code Form on magnetic disks is called SPL.
   - ***Worst Situation- No Controls :*** Create 2 serious forms of exposure
     - Access to program completely unrestricted.
     - So, Programs are subject to unauthorised changes.
   - ***A Controlled SPL Environment:*** Requires implementation of SPL Management System (SPLMS).
     - Controls 4 routine but critical functions:
       i) Storing Program
       ii) Retrieving program for maintenance
       iii) Deleting obsolete programs from library
       iv) Documenting program changes to provide audit trail
     - Mere presence of SPLMS does not guarantee program integrity. Specific Planning & Control Techniques required.
     - Control Techniques : *[Address most vulnerable areas & should be considered Min. SPL Controls]*
       i) Password Control
       ii) Separation Of Test Libraries [Password for production programs can be changed regularly & disclose on need to know basis]
3. Audit Trail & Management Report *[Most imp. are program modification reports] [Enhance mgmt. control & audit function]*
4. Program Version No. *[Evidence for identifying unauthorised changes to program modules] [Highlights unsupported documentation or unauthorised change]*
5. Controlling Access to Maintenance Command *[Used in emergency by highly authorised person]*
6. Message Sequence Numbering *[Automatic number inserted in each message by SPLMS]*

6. Computer Centre Security Control (Physical Security) [NOV 03, 00] [Complex & Situation Specific – Most effective measure is most costly]

1. Fire	2. Water	3. Energy Variations	4. Pollution Damage	5. Unauthorised Intrusion
[Automatic/Manual Fire Alarm, Fire detection equip. or fire extinguishers, sprinkler system, Halogen Gas (Cease Fire)] [Smoke detectors, Control Panel, Master Switches, Emergency exit fire station]	*[Outcome of Fire, cyclones, tornadoes] [Water proof, drainage system]*	*[Increase, Decrease, Loss of Power] [Voltage regulators, Circuit breakers, Battery backup Generation Plant]*	*[Dust, inadequate filtering of air] [Ensure dust free environment, cleaning regularly, vacuuming, Dust Collection Rugs]*	*[To steal or damage] [Use alarms, guards, Security Devices, Badge System]*

Contingency Measure to recover from or to prevent the Disaster there is DRP (Disaster Recovery Plan) *[To ensure normalcy restored in set time & minimum loss]*

General Components Of The DRP : Plans (ReBaTE) [MAY 01] **[May 05]**

1. Emergency *[Immediately after disaster] [Evacuation (move from one place to another) Procedures]*
2. Recovery *[Sets out full capabilities restored][Recovery Committee][Setting out priorities of recovery]*
   - i) *Inventory of hardware, software, system taken*
   - ii) *Criticality evaluated*
   - iii) *Application System hierarchy spelled out*
   - iv) *Selection of disaster recovery site [Optional arrangement considering systems availability & data security]*
   - v) *Formal backup agreement with another co.*
3. Back up *[At physically distant from original site]*
4. Test plan *[Identifies deficiencies in above]* Procedure for conducting DRP Testing:
   - i) *Paper Walk through [Trial run] [Documentation]*
   - ii) *Localized test [Imitate System Crash]*
   - iii) *Full Operational Test [Nearer to disaster conditions]*

1. Recovery & Reconstruction
2. Testing

Insurance (Types of Policies)

1. *Data Processing*
2. *Valuable papers & records*
3. *Business Interruption*
4. *Extra expense*
5. *Errors & omissions*

7. Internet / Intranet controls [Nov 02]

Exposures in Communication subsystem:

A. Component / Equipment Failure	B. Subversive / Destructive Threats
[Transmission can be disrupted, destroyed or corrupted and result in loss of databases & program] 1. Communication Line 2. Hardware 3. Software	1. Invasive Tap *[Can read & modify data] [Insert, Delete, Modify, Alter order, Duplicate, Deny, Fake Association]* 2. Inductive Tap *[Allows data to be read only]* Controlling Risk From Subversive (Destructive) Threats 1. Fire Wall [May 04] *[System that enforces control bet^n two networks]* i) Network Level Firewall *[Low cost, Low security] [Consists of Screening router which examines source & destination address]* ii) Application Level Firewall *[High Network Security, Extremely Expensive] [Run security applications called proxies]* 2. Controlling denial of service attack *[Three-way Hand Shake] [SYN packet – SYN/ACK – ACD]* 3. Encryption *[Private key encryption(Same key; DES) & Public key encryption (Two different keys){Public key (Encrypt)-published-Sender & Private key (Decrypt)-secret-receiver}] [Cipher text – Algorithm to convert clear text into coded equivalent]* **[Nov 04]** 4. Message Transaction Log *[Record User ID, time of access & telephone no. of originator]* 5. Call Back Devices *[User enter password & then system breaks connection to perform authentication]*

8. INHERIT PROBLEMS OF PERSONAL COMPUTERS & CONTROL **[May 03]**		
1. Weak Access Control a) Log on Procedures b) Disk Locks (Memory Resident *[Password controlled]* & Physical)	**2. Multilevel Password Control** a) Restrict employees sharing same PC b) Access control List o *Enhance small org^{n} control environment*	**3. Inadequate Backup Control** a) Floppy Disk Backup b) Dual Internal Hard Drives c) External Hard Drives (Zip Drives) *[Removable Disk Cartridge]* d) Tape Backup Drives (Internal or External)

Breach of Computer Security *(Physical, Software, Data, Data Communication)*	Accidental	*Fire, Water Damage, Energy Variation, Pollution, Unauthorized Assess*
	Incidental (Intentional)	*Fraud, Tampering, Malafide intention*

Types of Application Controls

(A) INPUT CONTROLS *[Ensure transaction are valid, accurate, complete]*

Various Classes of Input Controls: [Not Mutually Exclusive]

1. Source Document Controls

a) Use Pre numbered Source Document *[Unique Sequential No.]*
b) Use Source Document in Sequence *[Physical Security]*
c) Periodically Audit Source Document *[Reconciling Sequence No.]*

2. Data Coding Controls *[Check Digit Controls]*

Errors that corrupt data code & cause procession errors [May 04]

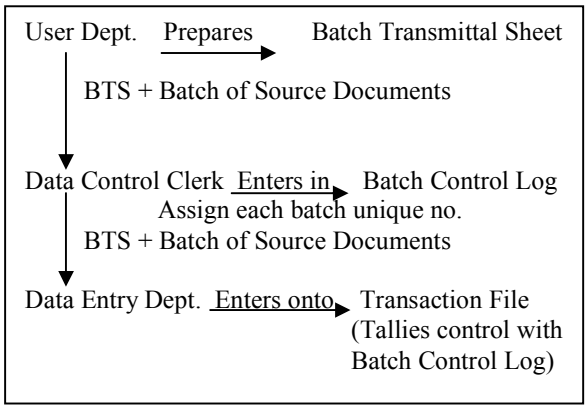
a) Transcription Errors *[To Write]*
   i) Addition Errors [Added]
   ii) Truncation Errors [Digit/Character Removed from end]
   iii) Substitution Errors [Replaced]
b) Transposition Errors *[Interchange]*
   i) Single Transposition [Adjacent digit are reversed]
   ii) Multiple Transposition [Non-Adjacent digits are transposed]

- Method of detecting Data Coding Errors *(Added to code when it is originally assigned)* : Check Digit Method *[11-Module Check digit-Best to detect transposition errors]*

3. Batch Controls *[Documents to reconcile output produced with inputs entered & grouping similar input transaction in batches][For high volumes of transaction data]*

Two Documents to accomplish the task:

a) Batch Transmittal Sheet
b) Batch Control Log



4. Validation Controls *[Detect errors in transaction data before data processed]*

a) Field Interrogation *[Programmed procedure that examine characters of data in field]*
   i) Limit Checks *[For Input & Output] [Value lies within limits] [Combination checks]*
   ii) Picture Checks *[Against processing incorrect characters]*
   iii) Valid Code Checks *[Against pre determined transaction codes, tables]*
   iv) Check Digits *[As in data coding controls]*
   v) Arithmetic Checks *[x/y=z or x=y*z]*
   vi) Cross Checks *[Tally Results]*

b) Record Interrogation
   i) Sequence Checks *[Detect missing transaction, erroneous sorting]*
   ii) Format Completeness Checks *[Checks presence & position of all fields]*
   iii) Redundant Data Checks *[in Sequential Processing]*
   iv) Combination Checks
   v) Passwords *[In online systems for processing inquiries]*
      - Cost Benefit Analysis
      - Different standards of control for error in:
        - Transaction File : One time error
        - Master File : Continuous source of error

c) File Interrogation *[To ensure correct file is Processed] [Imp. for Master File]*
   i) Internal Label Check *[Header/Trailer Label]*
   ii) Version Check *[Correct Version processed] [GPC Approach]*
   iii) Expiration Date Check *[Prevents deleting file before expiry]*

5. Input Error Correction

a) Immediate Correction *[In Direct Data Validation Approach] [System halt's data entry until user corrects error]*
b) Create an error file *[In Delayed Validation]*
   Batch control apply to re-submitted data
   i) Reverse effect of Partially Processed & Resubmit corrected records
   ii) Re insert Corrected records
c) Reject the Batch *[When error is associated with entire batch & not clearly attributable to individual records] [Eg: Imbalance in batch control total]*

6. Generalized Data Input System

(B) PROCESSING CONTROLS

1. Run-to-run Controls *[Ensure each run processes batch correctly & completely]*

Uses:

i) Recalculate Control Totals *[Fields(Financial Record/ Control Total), Hash Totals, Record Counts]*

ii) Transaction Codes *[Compared with transaction code in control record] [To ensure only correct type of transaction is processed]*

iii) Sequence Checks

2. Operator Intervention Controls

[Increases potential for human errors. Although impossible to eliminate operator involvement completely but, to extent possible, parameters value should be derived logically or provided through look-up tables]

3. Audit Trail Controls

Techniques Used to Preserve Audit Trails in CBIS

1. Transaction Logs *[Records successfully processed transaction]* [Nov 03] **[May 05]**
2. Transaction Listing *[Hard copy of successful transaction for reconciliation with Input]*
3. Log of Automatic Transactions *[Triggered internally by system] [Eg: Inventory falling below reorder point]*
4. Listing of Automatic Transactions
5. Unique Transaction Identifiers *[Transaction No.- For tracing particular transaction from whole record]*
6. Error Listing *[To support error correction & resubmission]*

(C) OUTPUT CONTROLS *[Ensure System output is not lost, misdirected or corrupted & privacy not violated] [Choice of control influenced by type of processing method in use]*

1. Controlling Batch Systems Output

[More exposed, so greater control]

a) Tape & Disk Output Controls [Storage]

- Built-in dual recording mode enable to check recording accuracy:
  - Comparison (ECHO Check)
  - Use file labels
  - Check file retention date
  - Incorporate output controls

i) Hardware [Parity bit checking]

ii) Software [Check digits]

b) Printed Output Controls [Printer] *[Pg. no., date, etc]*

i) Verification of Output

1) Directly related to input

2) Indirectly related to input

3) Exception Reports [Eg: Slow Moving stock]

ii) Distribution Of Output [Receive all o/p; intact]

iii) Procedures for acting on Exception Reports [Because imp. control functions are based; like control of overtime]

2. Controlling Real Time Systems Output

a) Exposure from Equipment Failure

b) Exposure from Subversive Acts

Computer Fraud Includes:

"Any illegal act for which knowledge of computer technology is essential for its perpetration, investigation or prosecution."

"Using a computer to cause prejudice in the sense of financial and/or reputational damage to a business" may be called a computer fraud. Computer fraud includes:

1. Clearly recognizable frauds *[Investment, Secret Market, Pyramid Schemes] [New medium to convey an old message]*
2. Hacking *[Unauthorised access/modification]*
3. Manipulation of Computer System to obtain money from an employer/third party *[collusive fraud] [Diversion of funds]*
4. Theft & Destruction of confidential & sensitive information *[Causes huge damage]*
5. Abuse of computer system by employees *[goofing]*
6. Software Piracy

Primary Risks to Business Organisation *[Extreme efforts to cause maximum damage]*

A. INTERNAL THREATS [Riskier Than External Threats] *[4 out of 5 frauds involves employees]*

Q. Categories of Computer fraud based on Data Processing Model

1. Input *[Little computer Skills]* [May 04]
   i) Collusive fraud *[Forged Deposit Slips]*
   ii) Disbursement fraud *[Fraudulent Bills]*
   iii) Payroll frauds *(Fictitious employees)*
   iv) Cash-receipt frauds *[Sales as half price]*
2. Processor *[Unauthorised system use; goofing]*
3. Computer Instructions *[Technical/specialised knowledge][Least common]*
4. Data *[Alter, damage, scramble, steal without authorization]*
5. Output *[Stealing or misusing O/p Displayed on monitor/Printed on paper]*
6. Malicious alteration of email *[Grudge against other employee]*

B. EXTERNAL THREATS

1. Hacking Threats
2. Information removal
3. Destruction of system integrity
4. Interference with web pages
5. Transmission of virus by email
6. Interception of email/e-payments
7. Internet Frauds **(U-GIGO)**

Steps to Detect Computer Frauds / Improve Detection Methods [Nov 02]

1. Conduct Frequent Audits *[External / Internal / Special Network Security Audit]*
2. Use a Computer Security Officer
3. Use Computer Consultants
4. Monitor system Activities *[Maintain & Review Logs] [Find weaknesses & suggest improvements]*
5. Use Fraud Detection Software

Preventing Computer Frauds / Reduce potential of Computer Frauds

1. Make fraud less likely to occur *[Employees are greatest control strength & weakness]*
2. Use Proper Hiring & Firing practices
3. Manage Disgruntled employees
4. Train employees in: **(FM-STE²PS)**
   a) **S**ecurity Measures *[Well-schooled]*
   b) **T**elephone disclosures *[Dialing the caller back] [Asking Penetrating & Specific ques.]*
   c) **F**raud awareness *[Aware of occurrence & dangers]*
   d) **E**thical considerations *[Promote in Practice] [Acceptable / Unacceptable Behaviour]*
   e) **P**unishment for unethical behaviour *[Warning, dismissal, prosecution, penalties]*
   f) **E**ducating employees *[In Security, fraud awareness, ethics otherwise consequences]*
   g) **M**anage & track software licenses *[Enough to meet user demand] [Protects from software piracy law suits]*
   h) **S**ign confidentiality agreements *[All employees, vendors, contractors to sign & abide]*

Risk to Internet Frauds / Attract Fraudsters (U-GIGO) [Nov 04, May 04]

1. **U**nregulated *[No License Fees]*
2. **G**lobal Reach *[At low cost] [Access to larger market of potential victims]*
3. **I**mpressive site with links *[empty shell designed to trap/attract innocent]*
4. **G**lamour & Novelty *[Bogus credibility cause cautious investor to be trapped]*
5. **O**utside legal jurisdiction

Reasons for risk in Computer Frauds / Rise in Computer Frauds (UN-LILI) [Nov 04]

1. **I**gnorance of law
2. **U**ndetected
3. **N**ot reported *[Adverse Publicity & B'coz of fear of copycat fraud & loss of customer confidence] [Reveals weakness of system] [Only banks required to report]*
4. **L**ow level of security *[Difficult, Costly, Time consuming to investigate]*
5. **I**nstructions on how to perpetrate computer frauds
6. **L**aw is unable *[Sentences very light]*

Controls to make Fraud difficult to perpetrate / Increase the difficulty of Committing Fraud

1. Develop a Strong System of Internal Controls *[Responsibility of Top Mgmt.] [Delegation]*
2. Segregate Duties
3. Require Vacations & Rotate Duties
4. Restrict Access to Computer equipment and Data Files *[Restrict Physical & Logical access]*
5. Encrypt Data & Programs
6. Protect Telephone Lines *[From Computer Phreakers] [Attach electronic lock & key]*
7. Protect the System from Viruses *[Use Latest version] [Detection good than protection]*
8. Control Sensitive Data *[Appropriate access restriction]*
9. Control Laptop Computers *[Impossible to boot up without password]*

COMPUTER FRAUD & ABUSE TECHNIQUES	
Technique	**Description**
Virus *[Viral Information Research Under Seize]*	Segment of executable code, attaches, replicates & spreads in system triggered by predefined event. Not always destructive. Difficult to trace its origin as grows geometrically. Destroys application program, data files, OS in no. of ways. Most dangerous aspect is its ability to spread before committing destructive acts.
Worm	Program that copies & actively transmits to other systems. Short life but quite destructive. It attacks unused space in RAM. Differs from virus – Replicated worm modules remain in contact with original worm that controls their growth while virus grows independently.
Logic Time Bomb	Program triggered by predetermined event. Once triggered, damages system.
Hacking	Unauthorised access by PC & telecommunication networking. They don't intend to cause any damage. Act of destroying/deleting/damaging/altering any info. residing in a computer resource inspite of knowing such action is likely to cause damage.
Cracking	Hackers with malicious intentions *[Delete, damage, destroy the system (program/files/data)]*
Password cracking	Intruder gains access by stealing password file
Trojan Horse	Accessing by copying others User ID.
Masquerading/ Impersonation	Perpetrator gains access by pretending to be authorized user. Enjoys same rights as legitimate user.
Super Zapping	Bypass regular system controls and perform illegal acts. Entering through bootable floppy drive.
Trap Door/Back Door	Entering using back door.
Eavesdropping	Listening to private voice using wire tap.
Piggybacking	Tapping into telecommunications line & latching on to a legitimate user before he logs into system as he unknowingly carries perpetrator into system.
War Dialing	Perpetrator enters the system through the idle modem & captures PC attached to it & thus its network.
Scavenging (Hunting)	Accessing to confidential info. of Corporate records from trashcans, carbon copies, history.
Denial Of Service Attack	Blocking Server by sending numerous mails (e-mail bombs). Email is overloaded & thus shuts down.
Round Down	Int. calculations rounded to 2 decimals & balance fraction is placed in a/c controlled by perpetrator.
Salami Technique	Tiny slices of money stolen over time *[Exps. increased by fraction]*
Internet misinformation	Spread false or misleading information through internet.
Internet Terrorism	Disrupt e-commerce & destroy communications through internet.

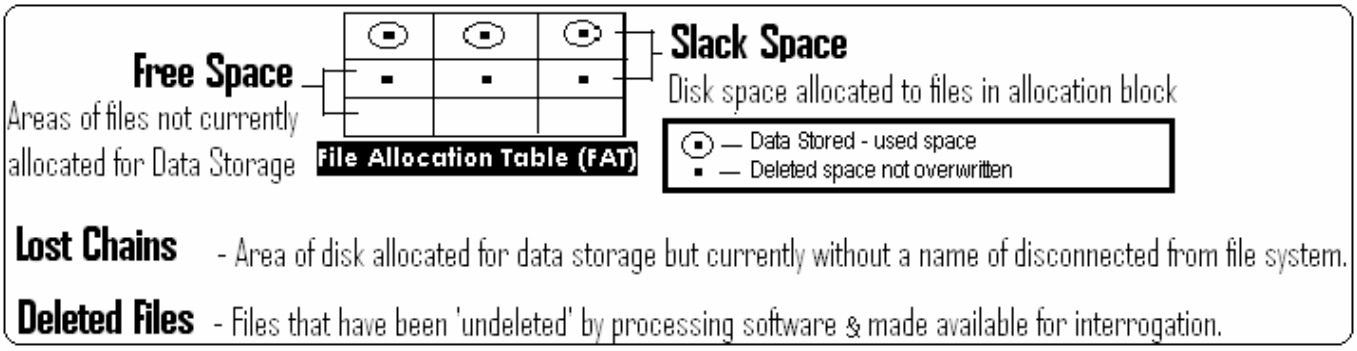
Data Diddling *[Modification/Alteration]*	Changing data before, during or after it is entered in system.
Data Leakage	Unauthorised copying of Co. data.
Social Engineering	Perpetrator tricks employee to get info. to get into system.
Software Piracy	Copy software without publisher's permission.
Spamming	Email same message to UseNet groups with threat
Email Forgery	Send email message as if send by someone else.
Email Threats	Send threatening message to make recipient to do something to cheat him.

METHOD OF DETECTION OF COMPUTER FRAUDS

Disk imaging & Analysis Technique *(Computer Forensic Tools)* **[May 05, 03]**

Stages: (For Single PC)

1. Exact copy of Computer Hard drive is taken leaving original completely intact.
2. Image copy of disk is processed. *[Areas of storage containing partially overwritten files & deleted but not overwritten files are recovered]*
3. Analysis of processed image. *[Programmed to find references to suspect transaction. Extent of search depends on software used.* Single word / Phrases / Number Search]



Cyber Laws and Information Technology Act, 2000

Not Applicable to negotiable instrument, power-of-attorney, trust, will, contract for sale or conveyance of immovable property or interest in such property, other documents or transactions notified by CG in OG.

Objectives: [May 05]

- Legal recognition of transactions carried out by EDI & E-Commerce
- Legal recognition to DS
- Legal recognition to Booking Keeping in e-form by bankers
- Facilitate e-filing / e-storage / e-funds transfer between Banks & FIs
- Amend Indian Penal Code, Indian Evidence Act, Bankers Book Evidence Act, RBI Act

Issues not covered by the Act:

- Protection for domain names
- Infringement of copyright laws
- Jurisdiction/Stamp duty aspects of e-contracts
- Taxation of goods & services traded through e-commerce

Chapter	Section	Description
I	1 & 2	Scope & Defination [May 03]
II	3	How to create DS / Authentication of E-Records using DS
III	4 to 10	Legal recognition given by government to DS / E-Governance
IV	11, 12, 13	Acknowledgement & Dispatch of e-records
V	14 to 16	Security procedure prescribed by government / Secure E-Records & DS
VI	17 to 34	Appointment & Power of Controller including Appointment & Duties of Certifying Authorities
VII	35 to 39	Issuance & Suspension of DSC
VIII	40 to 42	Duties of Subscribers
IX	43 to 47	Penalties & Adjudication
X	48 to 64	Cyber Regulations Appellate Tribunal (CRAT)/Presiding Officer (P.O.)
XI	65 to 78	Offences
XII	79	Network service providers not liable in certain cases, if proves offence committed without his knowledge/consent *[For third party info. available to him]*
XIII	80 to 94	Miscellaneous

Hierarchy of Authority

Central Government	Appoints Adjudicating Officer & Cyber Regulation Appellate Tribunal			
Controller	Delegate Deputy Controller, Assistant Controller or Other Officer			
Certifying Authority	Application for license: Fees ≤ 25000 *(With COP & identification stat.)* [Sec. 22]	Renewal: Fees ≤ 5000 [Sec. 23]	License Suspended ≤ 10 days	No revocation *(incorrect/ false particulars or contravention)* or rejection unless opportunity of being heard
Subscriber	Application for DSC: Fees ≤ 25000 (Prescribed by CG and different for different class of applicants) [Sec. 35]		DSC Suspended ≤ 15 days	

Digital Signature [Nov 04]	
Digital Signature Creation	Signed Message + Unique Hash Result + Private Key
	Authentication of electronic record by subscriber by electronic method in accordance with Sec. 3
Hash Result = Algorithm mapping/Translation of one sequence of bits into another, generally smaller.	
Asymmetric crypto System	System of secure **key pair**
	Private Key (create DS) + Public key (Verify DS)[Listed on DSC]
Code of Private key has to be in atleast 128 bits	

Digital Signature is created in two steps: [Ch II – Sec. 3] [Nov 02]

1. Convert e-record into message digest using Hash function to freeze e-record. *[To ensure integrity of content]*
   - *Any tampering with contents invalidate DS.*
2. Identity of person authenticated through private key.
   - *Verified by anybody who has public key corresponding to such private key.*
   - *Public Key enables anybody to verify whether e-record is intact or tampered & also Identify originator of message.*

Digital Signature Certificate ***[Like electronic passport]*** [Nov 03-5 Marks]

- Mechanism for authenticating and securing the information that is transmitted between two parties.
- Public key, with some identifying info, digitally signed by certificate authority.
- Identifies subscriber, certification authority, operational period & subscriber's public key.
- Ensures that purported sender is in fact the person who sent the message.
- Basic purpose to serve need of person seeking to verify DS to know :
  - *Public key corresponds to private key used to create the DS.*
  - *Whether public key is identified with signer.*

Appointment by Central Government

Person Authorised	Qualification	Further action by Aggrieved person
Adjudicating Officer *[To Adjudicate(act as judge) contravention]*	Director of Govt. of India or equivalent officer of SG *(Experience in IT & legal/ judicial)* Sec. 46	Appeal within 45 days from date of order recd. from Adjudicating Officer to CRAT
Cyber Regulation Appellate Tribunal *(Presiding Officer Only, for 5 yrs. Or 65 yrs. age, whichever is earlier)*	Judge of H.C. or Min 3 yrs. member of Indian legal service in Grade I	Appeal H.C. within 60 days from CRAT decision communicated (Sec. 62) *[On question of law or fact arising out of order]*

Penalty For Damage To Computer, Computer System Or Network [Ch. IX] [Sec. 43 to 45]

1. Securing unauthorized access.
2. Downloading or extracting any data, computer database or information.
3. Introducing any computer contaminant (toxin) or computer virus.
4. Damaging *(Destroy, alter, delete, add, modify, rearrange)* data, database or programme.
5. Disrupting.
6. Denying access to authorised person.
7. Providing assistance to any person in contravention of any provision.
8. Charging services availed by one person to the account of another by tampering with or manipulating.

Powers of Central Government	
1. Power to make rules in respect of DS a) Type of DS b) Format of affixing DS c) Procedure for identification of person affixing DS d) Control/Procedure to ensure integrity, security & confidentiality of e-records/ e-payments e) Any other matter to give legal effect to DS	Sec. 10 – Ch. III
2. Power to prescribe security procedures for e-records & DS	Sec. 16 – Ch. V
3. Power to appoint Adjucating Officer	Sec. 46 – Ch. IX
4. Power to appoint Presiding Officer	Sec. 48 – Ch. X
5. To declare any computer to be a protected system	Sec. 70 – Ch. XI
6. Power to make rules by notifying in Official & Electronic Gazzate (9 Pts.) [May 04]	Sec. 87 – Ch. XIII

Powers of Controller	
1. Grant recognition of foreign certifying authority	Sec. 19 – Ch. VI
2. Repository (Treasurer) of all DSC *[Computer database of all public keys, so that it is available to general public]*	Sec. 20 – Ch. VI
3. License to be issued to certifying Authority to issue DSC	Sec. 21 – Ch. VI
4. Cancel of license of Certifying Authority *[On grounds of incorrect, false particulars & contravention of Act]*	Sec. 25 – Ch. VI
5. Power to Delegate *[in writing]*	Sec. 27 – Ch. VI
6. Investigate contravention	Sec. 28 – Ch. VI
7. Access to any computer system if reasonable cause to suspect contravention	Sec. 29 – Ch. VI
8. Direction to certifying authority to take measures or cease carrying activities to ensure compliance of law	Sec. 68 – Ch. XI
9. To intercept any information transmitted through computer in public interest	Sec. 69 – Ch. XI
10. Power to make Regulations *[After consulting Cyber Regulation Advisory Committee after CG approval]*	Sec. 89 – Ch. XIII

Duties Of Certifying Authority [Ch. VI] [Nov 02]

1. Follow following procedures in respect of Digital Signatures : [Sec. 30]
   - Use of hardware, software & procedures that are secure from intrusion & misuse.
   - Provide a reasonable level of reliability in its services.
   - Adhere security procedures to ensure secrecy & privacy of DS.
   - Observes such other standards specified by regulation.
2. Ensure that every person employed by him complies provisions of Act/rules/regulations/order. [Sec. 31]
3. Display its license at a noticeable place in business premises. [Sec. 32]
4. Disclose its DSC containing its public key corresponding to private key used by him [Sec. 34]
5. No DSC shall be granted unless Certifying Authority is satisfied – **[Ch. VII]** [Sec. 35]
   - Applicant holds private key corresponding to public key issued in DSC which is capable of creating DS.
   - Public key listed in certificate can be used for verifying DS affixed by private key.

Duties Of Subscribers [Ch. VIII]

1. On acceptance of DSC, generate a key pair using a secure system. [Sec. 40]
2. Deemed to have accepted a DSC if publishit or demonstrates his approval & thus certi fies that - [Sec. 41]
   - Holds private key corresponding to the public key listed in DSC.
   - All representations made and all information in DSC is true.
3. Exercise reasonable care to retain control of the private key and prevent its disclosure to a person not authorised to affix the DS of the subscriber. [Sec. 42]
   - If Private Key is compromised (endangered / exposed) then communicate immediately to Certifying Authority, otherwise subscriber will be liable.

Powers of Cyber Regulations Appellate Tribunal [Ch. X]

1. Summoning & enforcing the attendance of any person & examining him on oath.
2. Producing documents & e-records.
3. Receiving evidence on affidavits (Sworn Statement).
4. Reviewing its decisions.
5. Issuing commissions for examination of witness.

Offences [Ch. XI] (THP CS GS CFP ICID)

Section	Offence (Fine or Imprisonment or both)	Max. Fine	Max. imprisonment
65	Tampering with computer source code documents *[Listing of programmes, computer commands, design & layout & computer resource in any form]*	2 Lacs	3 Yrs.
66	Hacking with Computer System	2 Lacs	3 Yrs.
67	Publishing Obscene info. in e-form o First Conviction o Second or Subsequent conviction	 1 Lacs 2 Lacs	 5 Yrs. 10 Yrs.
68	Power of Controller to give directions to Certifying Authority for compliance of law *[Non-compliance of Controller's Direction]*	2 Lacs	3 Yrs.
69	Directions of Controller to a Subscriber to extend facilitates to decrypt information *[Failure to assist]*	--	7 Yrs.
70	Govt. to declare protected system *[Securing access to protected system]*	√	10 Yrs.
71	Misrepresenting or Suppressing material fact from Controller or Certifying Authority	1 Lacs	2 Yrs.
72	Breach of Confidentially & privacy of e-records, books, info., etc. with out consent	1 Lacs	2 Yrs.
73	Publishing False DSC or otherwise making it available to other person	1 Lacs	2 Yrs.
74	Publishing DSC for Fraudulent Purpose	1 Lacs	2 Yrs.
75	Apply for offence committed o/s India *[If offence involves computer, computer system/network in India; irrespective of nationality]*		
76	Confiscation of Computer, CD, Floppies, Tape Drives or other accessories		
77	Penalty & confiscation under this act not Interfere with other prosecution under other act		
78	Power to investigate offences by Police Office ≥ DSP		

Issues of Primary Concern for auditor in IS Audit / Auditing Concerns [May 03]

1. Systems Controls *[Look total systems environment – not just computerized segment]*
   - *Involvement from initiation of transaction till posting*
2. Provisions made for:
   - *Audit trail for tracing forward & backward transaction*
   - *Ensure integrity of transaction*
   - *Handling exception & rejection*
   - *System perform as stated / Met predefined specification*
   - *Training User Personnel*
   - *Proper Authorization given*
   - *Adequate controls between interconnected computer systems*
   - *Adequate security procedures (Back up & recovery)*
   - *Operational platforms are compatible & controlled*
   - *Duplication is avoided & multiple databases updated constantly*
3. Safeguard organization assets [Primary Concern]

Factors that lead Manual Audit System Ineffective in IS Audit / Computer Auditing Approach **(EAT NR)**

1. Electronic evidence *[Not physically retrievable]*
2. Terminology *[Difficult to understand for Non EDP Auditor]*
3. Automated Process *[Difficult to understand for Non EDP Auditor]*
4. New Risks & Controls *[New for Non EDP Auditor]*
5. Reliance on controls *[Hard Copy evidence not available]*
   - Method of audit varies among org^n & applications.

Review areas where IS Auditor needs to Focus / IS Audit's Scope & Objectives **[To evaluate whether IS Audit is successful]**

1. Computerized Systems & Applications *[Appropriate to user's needs] [Efficient & adequately controlled to ensure valid, reliable, timely & secure I/p, Process, O/p at current & projected level]*
2. Info^n Processing Facilities *[Controlled to ensure timely, accurate & efficient Processing of Applications at normal & troublesome situation]*
3. Systems Development *[Meet objectives of org^n & satisfy users requirements] [Written, tested & installed in accordance with GAS for Systems Development]*
4. Management of IS *[Distribution as per authority]*
5. C/S, Telecommunications, Internet/Intranet *[Ensure controls on C/S & their network] [Same level of control assurance with special emphasis on two key Internet / Intranet Protocols : TCP/IP & HTTP]*

IS Audit Objectives [Nov 03]

1. **Computer Security** *[Overall Security of equipment, program, communications & data]*
2. **Program Development & Acquisition**
   - Mgmt. Authorisation & User Acceptance, Documentation, Thorough Testing
3. **Program Modification** [Application & System Software] *–Test on Surprise Basis, Logical Access Controls*
   Techniques to test unauthorised program changes:
   a) Source code comparision program *[Compare current version with original source code]*
   b) Reprocessing Technique *[Uses a verified copy of source code; on surprise basis]*
   c) Parallel Simulation *[Similar to reprocessing except writes a program instead of saving verified copy of source code; Used to test during implementation process]*
4. **Computer Processing Controls [May 05]** *(Processing transactions, files, reports, other Computer records) [Objective : Processing/Updating of files /database & generate output] - Internal & External File Labels, Batch Totals, Erroneous Code*
   Techniques to test processing controls:
   a) Processing Test Data *[Processing hypothetical series of valid & invalid transaction(each & every possibility)]* **[Nov 04]**
      Resources of preparing Test Data: *[In batch processing & online system]*
      i) Listing of actual transaction
      ii) Test transaction used by programmer
      iii) Test Data Generator Program [Automatically prepares test data based on program specifications]
   b) Concurrent Audit Techniques [Nov 02, **04**] *[For monitoring online processing system]*
      i) Integrated Test Facility (ITF) [Fictitious file is created and test transactions are processed with live data] [May 04]
      ii) The Snapshot Technique [Nov 02]
      iii) System Control Audit Review File (SCARF) [May 03]
      iv) Audit Hooks [Real Time notification] [Helps auditor handle situation before the error or irregularities of out of control]
      v) Continuous & Intermittent Simulation (CIS) [Uses DBMS to trap exceptions]
   c) Analyze Program Logic *[For searching erroneous / unauthorized code]*
      - *When auditor suspects that 'Application Program' contains an unauthorized code or serious errors, detailed analysis of program logic in necessary*
      - *It should be used as **last option,** as it is time consuming & requires program language skill*

      Software Packages aids in analysis:
      i) Automated flowcharting programs [By interpreting program source code]
      ii) Automated Decision Table Program [Generates decision table representing program logic]
      iii) Scanning Routines [Search a program]
      iv) Mapping Programs [Identify unexecuted program code]
      v) Program Tracing [Sequentially prints all application program steps helps auditor detecting unauthorized program instructions, incorrect logic paths & unexecuted program code]
5. **Source Data Controls** – *Input controls Matrix, Independent function*
6. **Data Files** – *Auditing by Objectives, checklist*

Disadvantages of Test Data Processing

1. Spend considerable time for understanding system & preparing test data.
2. Care must be taken to ensure that test data does not afford cos. Files & databases.
3. Reversal procedures (of test data) may reveal existence & nature of auditor's test to key personnel.

Concurrent Audit Techniques

- Used when in online system it is difficult/impossible to stop system to perform audit tests. It continually monitor the system while live data are processed & use **embedded (included) audit modules***(Performs audit function, report test results & stores evidence for Audit Review).*
- Time consuming & difficult to use but are so if incorporated when programs are developed.

1. Integrated Test Facility

- Places small set of fictitious records in master file
- Processing test transaction to update these dummy records will not affect actual records
- Distinguish ITF records from actual records, collects info. on the effects of test transaction & report the result
- Well suited for online processing systems as test transaction can be submitted on frequent basis, processed with actual transaction & traced throughout every processing stage
- Accomplished without disrupting actual processing, but take care not to combine dummy & actual during reporting

2. The Snapshot technique

- Examines the way transactions are processed
- Selected transactions are marked with special code (that triggers snap shot process)
- Audit modules are included in the program
- Snapshot data are recovered in a special file & then reviewed

3. System Control Audit Review File

- Uses embedded audit modules to continuously monitor transactions activity
- Collect data on transactions with **special audit significance***(exceeding specific amount, inactive accounts, deviating from cos. policy)* and recorded in SCARF File or Audit log
- Periodically takes print out, examines questionable transactions & performs necessary follow up

4. Audit Hooks (Trap for catching) / Real-Time Notification

- Audit routines(programs) that flag(mark) suspicious transactions
- Internal Audit dept. is notified when tagged transactions is associated with withdrawal/fraud

5. Continuous & Intermittent Simulation

- Embeds audit module in DBMS that examines all transactions that update the DBMS
- If transactions has special audit significance, module independently processes data like in Parallel Simulation
- Records results & Compares
  - If discrepancies – written on audit log for subsequent investigation
  - If serious discrepancies – CIS may prevent DBMS from executing update process

IS Audit Framework for Computer Security to meet Objectives [May 04]				
Types of Error & Fraud	Control Procedures / Actions to be taken *{To minimize security errors & frauds}*	System Review : Audit Procedures *[Review, Examine]*	Test Of Controls : Audit Procedures *[Verify, Reconcile, Evaluate adequacy, Observe]*	Compensating Controls *{Balancing}*
o Theft / Accidental / Intentional damage to hardware & files o Loss / Theft / Unauthorized access / modification / use to program & data files o Loss / Theft / Unauthorized disclosure of confidential data	o Logical access controls – password protection & authentication procedures o File back up & recovery procedures o Data Storage & transmission controls (Encryption) o Disaster Recovery Plan (DRP) o Information Systems Insurance o Information Security / Protection Plan o Restriction on Physical access to computer equipment o Virus Protection procedures o Firewalls	o Logical access policies o File back up & recovery policies o Data storage & transmission policies o Examine DRP o Examine casualty Insurance Policies o Interview IS personnel about security procedures o Written documentation about physical access policies	o Records of Password assignment & modification o Observe preparation & off site storage of backup files o Extent of data encryption use & effective use of data transmission controls o Examine the results of DRP o Limitation & amt. of Insurance coverage o Effective use of firewalls / protection procedures	o Sound personnel policies o Effective user controls o Segregation of incompatible duties

Various information can be gained by asking following questions: Standard Yardstick
What, Why, When, Where, How, Who

IT Resource, IT Process, Information

Sensitive Information:

1. Strategic Plans *[Crucial to cos. success] [In today's global environment, the advantage of achieving insight in to competitors intentions can be substantial]*
2. Business Operations *[Includes organization processes & procedures(like price list); Carelessness can result in compromise]*
3. Finances *[Salary, Wages]*

Establishing better Information Protection *[Factors for deciding level of protection]*

1. Not all data has the same value *[Holds vast array of data; gives priority]*
2. Know where critical data resides *[Management by exception]*
   - *To establish an integrated security solution*
   - *Provides significant cost benefits, as co. does not spend more on protecting data than data's worth*
3. Develop an access control methodology *[Password]* / Associated Auditing
   - *For imp. data, extend to file level. To prevent from info. unintentional damage, disclosure or copying leaving data useless.*
4. Protect info. stored on media *[FD, CD]*
5. Review hard copy output *[Recycle bin, thrash, containers]*
   - Protecting info. must be done with appropriate level of security at a cost that is acceptable to business.

Security Objective

"Protection of the interest of those relying on information, information system & communications that deliver the information from harm resulting from failures of availability, confidentiality and integrity *[Priority & Significance varies]*."

Ground Rules for design & implementation of Information Protection *[Address sequentially]*

1. What information is & Where located
2. Value of information & how difficult to recreate, if damaged or lost
3. Who is authorized to access & permitted to do what. [Rights]
4. How quickly information made available, if unavailable for any reason [Speed of Retrieval]

Types of Information Protection / Protecting computer held information

1. Preventive Info. Protection
   - Security Control: 1. Physical *[Access lock, CCTV, guards]* 2. Logical/Technical *[Password, A/c privileges, Access control list]* 3. Administrative *[Security awareness]*
2. Restorative Info. Protection *[Prevention after mishap] [Timely info. backup & recovery is vital]*
3. Holistic Protection *[Protection of organization as a whole at acceptable cost] [Expect worst event to happen]*

Core Principles of Information Security [M^2ATRICS] [May 05, Nov 03]

1. **A**ccountability	To define accountability & responsibility *[Remedial Measures]*
2. **A**wareness	To create an awareness of the risks & need for security *[On-going Process]*
3. **M**ultidisciplinary	To consider technological & non technological issues *[Adm., Oper., Orgn., Legal issues]*
4. **C**ost Effectiveness	To make security cost effective *[Safeguards, Balancing cost & risk]*
5. **I**ntegration	To coordinate & integrate security *[Integral part of overall management]*
6. **R**eassessment	To assess and re-assess periodically *[Changes; New threats]*
7. **T**imeliness	To provide for monitoring & timely response *[in proportion with risk; Real time/After the fact]*
8. **S**ocietal Factors	To promote ethics by respecting the rights & interests of others

Information Security Policy / Security Implementation / Best Approach to implement Information Security

1. Definition of Security Policies *[Acceptable behavior; Not unique(differ from orgn to orgn); To prevent loss & save money]*
2. Development of Policies *[Support existing orgn policies; Securities]*
3. Defining roles and responsibilities *[For security to be effective; clearly communicated & understood]*

Role	Responsibility
Executive Mgmt.	*Overall*
IS Security Professionals	*Design, Implementation, Management & Review of orgn SP SMPP**
Data Owners	*Determining Sensitivity, Maintaining Accuracy & integrity of data*
Process Owners	*Ensuring appropriate security consistent with orgn SP SMPP*
Technology Providers	*Assisting with implementation*
Users	*Following set-out procedures*
IS Auditors	*Providing independent assurance on : Security objectives & SP SMPP comply*

4. Design of Security & Control Framework *[New & improved SMPP]*
5. Implementation of Security system *[On timely basis]*

Controls	To Ensure
Managerial	*Segregation of duties, training, education*
Identification & Authentication	*Passwords*
Logical Access	*Access control list*
Accountability	*Management audit trails*
Cryptography (key pair)	*Confidentiality, authenticity, integrity*
SDLC Process	*Security as integral part of process*
Physical & Environmental	*Fire Detection, Physical security*
Computer Support & Operations	*User support & software support; Documentation & Maintenance*
Business Continuity Planning	*Prevent interruption & resume processing*

6. Monitoring *[Subject to change & new risks; Promptly identify damage & accelerate recovery]*
7. Remedial measures
8. Awareness, Training & User Education *[Critical for success]*

*SP SMPP = Security Policy Standards, Measures, Practices, Procedures

Questions with similar topics	
Ch:13 Threats to System: Operating System Controls(1)	Ch:15 Threats to Business: Internal Threats & External Threats
Ch:13 Audit Trail Objectives: in Operating System Controls(1) Ch:13 Audit Trail & Management Report: System Maintenance Controls(5)	Ch:14 Audit Trail Controls: in Processing Controls : Techniques Used to Preserve Audit Trails in CBIS
Ch:14 Transaction Logs: in Audit Trail Controls	Ch:13 Transaction Logs: in Back up control in DBMS in Data Mgmt. Controls(2)
Ch: 13 Backup Control in PCs control(8) Ch: 13 Backup Control in DBMS(2)	Ch: 13 Back up Plan in General Components of DRP (REBATE) : Physical Security(6)
Ch:13 Equipment Failure & Subversive Threats Exposures in communication subsystem : in Internet/Intranet Controls(7)	Ch:14 Controlling Real Time System o/p in Output Controls

Questions not contained in notes	
Ch: 06	Benefits of C/S? May 04 Server Centric Model. M. 6.10
Ch: 13	Controls necessary in online & data communication system. Nov 99 Measures to be taken by Top Management/Computer Dept. to protect data (data security) & program/software. Nov 98
Ch: 15	Why should business take computer frauds seriously M.15.3. Nov 03, May 05
Ch: 17	Frameworks 2 to 6
Ch: 18	Role played by information security administrator. M. 18.20 May 03 Information Security & its importance May 04