Short Summary of

Information System Control and Audit (ISCA)

Group 2, Paper 6

CA Final

Before going through SHORT NOTES,

- Short Notes are based upon Study Material as provided by ICAI
- Go through Study Material as provided by ICAI.
- For Chapter 10, refer the Information Technology (Amendment) Act, 2008 for better clarification,
- I has not covered mostly topics from chapter 3 and some from other chapters too. Do not worry about them, they covers only 5-10 marks. Below content covered almost 90% of syllabus.
- I has mentioned only heading as the same are self explanatory after reading ICAI module once.
- Do No confuse with Para No. as mentioned at 4th column. It was originally page number for my reference, and for cross reference in certain topics (you will find "refer Para __").
- **Please appreciate other works and do not treat it as like that. Give your feedback on my mail-ID.**

Best of Luck

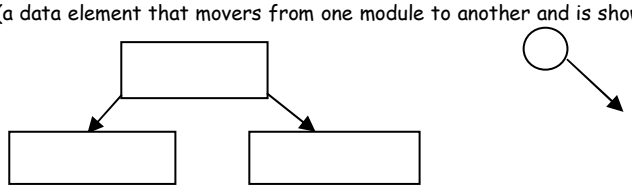
Arvind Sharma
09582089920

S. No.	Topic/Particulars	Description	Para No.
	Chapter – 1	**Information System Concept**	
1.	System Meaning	System may be defined as a set of interrelated and independent elements which works together to achieve predetermine objective.	1
2.	Type of System	Open and Closed or Abstract and Physical or Manual and Automated or Probabilistic and Deterministic	1 – 2
	Dif. b/w Open & Closed System	Basis of difference – Meaning, Life, Automatic Updates, Effectiveness, Interaction with Environment.	34
3.	System Concept	a) System Environment (set of elements which are out of concern & separated by system boundary) b) System Boundary (something which separate system from its environment) c) System Entropy (tendency of system toward disorder) and Negative Entropy (solution to bring back system to its normal condition) d) Sub-system (means that element of system which satisfy the meaning of system)	2 – 3
4.	Sub-system Concept	a) Decomposition or Factoring (breaking of system into components on the basis of functions) b) Simplification (i.e. management of interfaces amount sub-systems) c) System De-coupling (introduction of memory/buffer/store between two tightly couples sub-system to ensure smoothing functioning) d) Supra-system (i.e. a sub-system when refer by its sub-subsystem, like boss of employees) e) System Stress (i.e. stress feel by sub-system on over work by supra system)	3 – 8
5.	Information Meaning	Information may be defined as processed data which has meaning/use for its user.	9
6.	Attributes of Information	1) Relevant, 2) Mode and Format, 3) Comprehensive, 4) Availability, 5) Updated, 6) Complete, 7) Transparent and 8) Value Added	9 – 10
7.	Characteristics of type of information used in executive decision making.	Features of Executive's Information 1) Future Oriented, 2) Lack of details (Summarized), 3) Informal Source. 4) Lack of Structure (unstructured) and 5) Lack of Certainty (Uncertain)	10 – 11
8.	Factors affects Information Requirements	a) Level of Operation (Operative, Tactical or Strategic) b) Type of Problem or decision (Un/semi-structured or Structured) c) Level of Management (Top, Middle or Lower)	11
9.	Information System Meaning	A system which is intended to service information on requirement.	12
10.	Implication of IS in business	1) Help in decision making, 2) Help organization to gain edge in competitive environment, 3) Knowledge gathering through IS, 4) Help in taking right decision at right time.	12
11.	Computer Based IS (CBIS)	An IS which is computer enabled.	12
12.	Advantages of using CBIS or Computerized MIS over manual system	1) (Handle) Large Volume of Data, 2) Speedy Processing, 3) Quick Data Retrieval, 4) Widened Scope of Analysis 5) (More) Comprehensive Information, 6) Increase Effectiveness of IS 7) Integrate Sub-systems 8) (More) Accuracy in Output, 9) Cost Effective (low Cost of processing), 10) Flexible and User Friendly,	13
13.	Characteristics of CBIS	1) Predetermined Objective, 2) Sub-system concept based 3) All sub-system works together 4) Failure of one sub-system will cause entire system shut-down, 5) Common goal of system at top priority over individual goal of sub-system,	13
14.	Types of IS	a) Operation Support System (OSS – TPS, MIS and ERP) b) Management Support System (MSS – DSS, EIS/ESS and ES) c) Office Automation System	14
15.	Transaction Processing System	TPS is a IS which works at lowest level of management for processing routing data and generating routine information.	15 – 16
	1) What TPS do..?	a) Capture data (i.e. data entry) and organize them, b) Processing of data captured (using application software), c) Generation of Information in the form of Reports (routine reports) d) Processing of queries from various users (i.e. information on demand)	
	2) Component of TPS	1) Input (to capture data or queries) 2) Application Software or Processer (for processing or data retrieval) 3) Storage (to store captured data or/and processed information) 4) Output (to serve processed data or answer to queries)	
	3) Features of TPS	a) Large Volume of Data b) Automatic c) Output is measurable (i.e. quantitative output) d) Source of Input for other IS	
16.	Management IS (MIS)	MIS is an extension of TPS which, in addition to providing routing information, provides exceptional reports for management consideration.	17 – 21
	1) Characteristics of MIS	1) Management Oriented (request for development by management) 2) Management directed (active participation of managers in development) 3) Integrated (all functional system are integrated with it) 4) Common data flow (common input, processing, output and retrieval flow for all) 5) Common database (to avoid data redundancy) 6) Sub-system Concept (MIS should be developed in modules approach. In other words, there should be sub-system of MIS that have their own individual goal) 7) Computerized 8) Heavy Planning Element (since MIS intended for long run, there must be proper planning before development)	

	2) Pre-requisite for an Effective MIS	1) Management Support, 2) Expert System and Management Staff, 3) Common Database, 4) Regular Maintenance & Control and 5) Evaluation at regular intervals.	
	3) Benefits of using Computerized MIS - Refer advantages of CBIS at **Para 13**		
	4) Limitation of MIS	1) Do not deals with semi-structured or unstructured problems, 2) Consider only quantitative factors & ignore Qualitative inputs, 3) Quality of output depends upon quality of inputs, 4) Cannot provide tailor made reports for every type of problem, 5) Effectiveness get reduce over time due to change in management, 6) It cannot substitute the ability of management for taking decisions (i.e. MIS is not a decision making IS, but it assist in decision making) and 7) It does not have enough flexibility to update itself with changing needs of management.	
	5) Misconception about MIS	1) More input means more output 2) MIS can be computerized only 3) 100% Accuracy top priority (partially true, like in case of medicine industries)	
17.	Decision Support System (DSS)	- DSS is software based IS which help management to take decisions at right time. - It can be defined as a system that provides tools to managers to assist them in solving semi-structured and unstructured problems in their own way. - DSS support the human decision-making process, rather than providing a means to replace it.	22 – 25
	1) Characteristics of DSS	1) Deals with semi-structured or unstructured decision making, 2) Enough flexible to update itself to respond changing needs of manager/decision maker, 3) Easy to use	
	2) Component of DSS	1) User (with unstructured or semi structured problem) 2) Programming language 3) Database and 4) Model base	
	3) Application of DSS	Some example of DSS are as below:- 1) Cost Accounting System (to ascertain cost of product and price fixation) 2) Capital Budgeting System (to evaluate various investment proposal wrt assets) 3) Budget Variance Analysis System (to fix standards, find variance and evaluate the reason thereof) 4) General Decision Support System (to solve day to day structured problems)	
	- Programmed Decisions	- Programmed Decisions are those decisions which are of repetitive and routine nature. - It refers to decisions made on problems and situations by reference to a predetermined set of solution. - Such decisions are related to those problems which can be predicted in advance and solution can be made in advance. - Such decisions are made to solve structured problems and thus also called structured decisions	
	- Non-programmed Decision	- Non-programmed decisions are those decisions which related with unexpected problems and situation. - These are of non-repetitive and unexpected nature. - Such decisions are made wrt semi-structured decisions or unstructured problems.	
	- Database Architecture	Database architecture (to be distinguished from DBMS architecture) may be viewed, to some extent, as an extension of **Data modeling**. It is used to conveniently answer requirements of different end-users from a same database. For example, a financial department of a company needs the payment details of all employees as part of the company's expenses, but not other many details. Thus different departments need different *views* of the company's database that both include the employees' payments, possibly in a different level of detail (and presented in different visual forms). To meet such requirement effectively, database architecture consists of three levels.	
	- Three Level of Database Implementation	▪ The **external level** defines how each end-user type understands the organization of its respective relevant data in the database, i.e., the different needed end-user views (actual external view of required information over the screen as per user discretion). ▪ The **conceptual level** (or Logical level) combines the various external views into a coherent whole, global view. It provides the common characteristic of all the external views. It comprises all the end-user needed generic data, i.e., all the data from which any view may be derived/computed. It is provided in the simplest possible way. It is out of the scope of the various database end-users & serves database application developers and defined by DB admin that build the database. ▪ The **Internal level** (or Physical level) is a part of the database implementation/arrangement of data inside a DBMS in hard disk or storage media.	
	- Data Modeling	Data modeling in software engineering is the process of creating a data model for an information system by applying formal data modeling techniques. A data model can be thought of as a diagram or flowchart (i.e. an abstract model) that illustrates the relationships between data. Data modeling is the formalization and documentation of existing processes and events that occur during application software design and development. Well-documented models allow stake-holders to identify errors and make changes *before* any programming code has been written.	
18.	Executive IS (EIS)	EIS is a DSS which is designed and developed to meet executive's need and requirements.	26 – 27
	1) Characteristics of EIS	1) EIS is a CBIS, 2) EIS serves information needs of top executives, 3) EIS enables executive to extract required information from given output (report) without having	

		knowledge of query language, 4) EIS is capable of accessing both internal and external information, 5) EIS provides rapid access to timely information and direct access to management reports, and 6) EIS provides extensive online analytical tools.	
	2) Types of decisions taken by Executives	Most Executives decision falls into one of following category 1) Strategic Planning (it covers all such decisions which are for long term effects, e.g. major buy, new product launch etc.) 2) Tactical Planning (it covers decisions relating to day to day business operations, e.g. salary payment, vendors evaluation etc.) and 3) Fire Fighting (it covers decisions taken for immediate effects)	34
	3) Contents of EIS There is no prescribed list of contents of EIS. It may comprise all such components as Executive requires having.	Set of principles to guide design of Measures and Indicators to be included in an EIS:- 1) EIS measures must be easy to understand and collect. 2) EIS measures must be based on a balanced view of the organization's objectives 3) Performance Indicators in EIS must reflect contribution of everyone in a fair & consistent manner, 4) EIS information must be available to everyone in the organization, 5) EIS measures must encourage organization's staff to share ownership of the organization's objectives and 6) EIS measures must evolve to meet the changing needs of the organization.	
	- Purpose of EIS	1) Managerial learning, 2) Timeliness (i.e. timely access to information), and 3) Management attention (toward KPIs, new opportunities and problems) 4) Evaluating KPIs (key performance indicators) and 5) Problem identification and their solution	
	- Working of EIS	Step 1) Access Internal and External information, Step 2) Processing of information, Step 3) Quantitative and Qualitative analysis of processed information, Step 4) Result – is new opportunity or problem identified..? If yes, report to executive, otherwise, again step 1.	
19.	Difference b/w EIS and Traditional IS	Basis of difference – Level of Management or User, Source of Input, Purpose, Drill down facility, Format of Output and Interface	28
20.	Expert System (ES)	An expert system (also called knowledge based system) is an artificial intelligent system that applies reasoning capability to make a decision. An expert system is usually built (developed) for a specific area of problem called Domain.	29 – 32
	1) Characteristics of ES A characteristic of ES is the ability to declare or explain the reasoning process that it uses to make decision.	Following factors must be considered while developing an ES:- 1) Availability (application should work as per the organizational needs and its requirements) 2) Complexity (able to handle complex problems unlike other IS) 3) Domain (problem area, should be relatively small and limited) 4) Expertise (it should posses knowledge, dynamic and intuition) 5) Structure (must be able to cope with un-structured, uncertain, missing and conflicting data)	
	2) Business Application of ES	1) Accounting and Finance (it provides tax advice and assistance.) 2) Marketing (it provides decisions relating to marketing, e.g. sales price fixation, response to customer's problems etc.) 3) Manufacturing (it helps in manufacturing process in optimum utilization of resources) 4) Personnel (it provides decision wrt HR, their cost-benefit evaluation, other issues) 5) General Business (it provides day to day operation decision making, unexceptional decision making)	
	3) Need for ES (computerized)	1) Human experts are costly to hire, 2) No meter how much human experts are knowledgeable, they can handle only few task at a time, 3) Human experts have natural limitation of feeling fatigue, being tired etc.	
	4) Benefits of ES	1) ES preserve knowledge for long time unlike a human expert 2) ES respond at real time (i.e. never show being busy with otherwise), 3) ES assist beginners to think like a professional do, 4) ES are not subject to such human feelings as fatigue etc., 5) ES can handle various tasks at a time varying on subject.	
	5) Component of ES	1) User (the person having problem with self, who require expert advice), 2) User Interface (for interaction b/w user and Expert system, 3) Inference engine (it is the main processing element consisting of programs that request data from users, manipulates the KB and provide a decision to the user.), 4) Knowledge Base (i.e. storage/database of expert opinions, rules and assumption of system.) 5) Knowledge Acquisition Sub-system (it is that software component of ES that enable the Knowledge Engineer for updating KB by acquiring human knowledge)	
21.	Office Automation System		33
	1) Task performed by OASs	1) Document Capturing, 2) Document Creation, 3) Receipts and Distribution, 4) Filling, Retrieval, Search and Follow-up, 5) Calculations and 6) Recording Utilization of Resources	
	2) Benefits of OAS	1) Improve Communication, 2) Reduce Cycle time, 3) Reduce Office Maintenance Cost, and 4) Ensure Accuracy	
	3) Categories of Computer Based OAS	1) Text Processor and related systems 2) Electronic Document management system 3) Electronic massage communication system and 4) Teleconferencing and Videoconferencing System	

	Chapter – 2	**System Development Life Cycle**	35 – 125
1.	Reasons of Failure to achieve SD Objectives	1) Changing Users Needs (shifting user's need), 2) New Technologies (Lack of knowledge of New technology), 3) Resistance to change, 4) Lack of Senior Management Support, 5) Lack of User's participation, 6) Inadequate testing and user's training	35 – 36
2.	Role of Accountants in SD (RW)	a) As a Concurrent Auditor, b) Post Implementation Review and c) General Audit	37
3.	System Development Methodology	SD methodology is a formalized, standardized documented set of activities used to manage a system development project.	38
	Characteristics of SD Methodology	1) Entire project is divided into number of identifiable process/steps, 2) Proper documentation of every work undertaken, 3) Participation of Users, Managers and Auditors in System Development, 4) Proper testing of system prior to implementation, 5) Training plan for Operators & Users, 6) Post Implementation Review	38
4.	System Development Approaches	1) Waterfall 2) Prototype 3) Incremental 4) Spiral 5) Rapid Application Development 6) Agile	
5.	SD Life Cycle		
	Advantages of SDLC	1) Better planning and control by project managers, 2) Compliance to "prescribed standards" ensure better quality, 3) Documentation, 4) The phases are important milestones & help the project manager & the user for review & sign-off.	39
	Advantages of SDLC from the prospect of IS Auditors	1) The IS Auditor can have clear understanding of various phases of SDLC from detailed documents maintained during SDLC, 2) The IS Auditor can state in his report about compliance by project manager, 3) The IS Auditor can be a guide during the various phases of SDLC, 4) The IS Auditor can provide an evaluation of the methods & techniques used at various phases of SDLC.	40
	Shortcomings of the SDLC	1) The development team may find it cumbersome (weighty), 2) The user may find that the end product is not visible for long term, 3) The rigidity (inflexibility) of approach may prolong (extend) the duration of project, 4) It may not be suitable for small & medium sized projects.	
	Phases in SDLC	1) Preliminary Investigation, 2) System Requirement Analysis, 3) System Design, 4) System Acquisition and Development, 5) System Testing, 6) System Implementation/Changeover, 7) Post Implementation Review and System Maintenance	41
6.	Preliminary Investigation	The purpose of PI if to evaluate the project request. PI relates to collection of information to evaluate the merits of the request for new system and make a judgment about the feasibility of the proposed project.	42 - 48
	Objectives of PI	1) Clarify and understand the project request (Identification of Problem), 2) Determine the size of the project (Determination of Scope), 3) Determine the technical and operational feasibility of alternative approach (Feasibility Analysis), 4) Access cost and benefits of alternatives (Economic Feasibility) and 5) Report findings to the management with recommendation (Report to Management).	
	1) Identification of Problem	Evaluation of request for new project, determining genuineness of the same.	42 - 43
	2) Identification of Objective	Determine what type solution is required.	43
	3) Determination of Scope (i.e. identification of required solutions)	What proposed solution should accomplish at least to solve problem identified. Following questions are answered under this step:- 1) Functional Requirement, 2) Data to be processed, 3) Control Requirement, 4) Performance requirement, 5) Constraints, 6) Interface and 7) Reliability requirement Methods help in analysis of Scope a) Reviewing Internal Documents b) Conducting Interviews (Also known as **Methods of PI** which System Analyst uses to collect information) Factors to be kept in mind while searching for required solution. 1) Different users will represent different problem and required solution in different ways. The system analyst should elicit the common problem and solution from the initiator of the project (i.e. the person who originally request for new system). 2) Initiator may be a member of management while the actual user/operator may be from operation levels. An understanding of their (i.e. user) profile will help in designing appropriate user interface features. 3) The development team should clearly quantify the economic benefits. 4) Although economic benefits are critical factor for selecting a solution, other factors should also be	44 - 46

		considered. 5) Understand the impact of solution on organization. Solution which has wide impact are likely to meet with greater resistance.	
	4) Feasibility Study	1) Technical (is required techniques are available) 2) Financial (is the solution viable financially) 3) Economic (is benefits more than cost) 4) Legal (is solution valid in legal terms) 5) Resources (are human resources redundant (unnecessary) for the solution)	47
	5) Report to Management	At the end of this phase, System Analyst made a report and submit it to management for further consideration and reply about which solution should be adopted.	48
7.	System Requirement Analysis	In this phase of SDLC, users' expectations are identified.	49 - 57
	1) Collection of Information	To determine user's needs. Such information are collected by using some techniques know as **Fact Finding Techniques**. Fact Finding Techniques 1) Documents 2) Questionnaires 3) Interviews 4) Observations	50 – 51
	2) Analysis of Present System	When analyzing the present system, the following areas should be studies in depth (functional areas of present system which needs to be analysis by system analyst:- 1) Review of historical aspects, 2) Analysis of Input, 3) Analysis of Data files maintained, 4) Review of methods, Procedures and Data Communication, 5) Analysis of Output and 6) Review of Internal Controls After analysis/review as above, a) Model the existing physical & logical systems – under this step, SA • Properly document above analysis and reviews, • Depict the logical flow of present system through **system flow charts**, • Use **data flow diagram** to show the physical flow of existing system, • Compile **data dictionary** for the new information system. After completion of above investigation about present system, finally, SA should investigate & analysis, in depth :- 1) Present Work Volume, 2) Current Personnel Requirement and 3) Present benefits and cost.	52 - 55
	3) System Analysis of Proposed System	Under this step, required specification for proposed system are determined, which are as below:- 1) Input, 2) Database, 3) Methods, Procedure and Data Communication, 4) Output and 5) Work Volume	56 – 57
	4) System Requirement Specification Report - A report prepared by SA at end of this Phase of SDLC.		57
8.	System Design	System design involves first logical design and then physical construction of a system. The design phase involve following steps:-	58 -
	1) Architectural Design	It deals with arrangement of application in terms of hierarchy of modules and sub-modules. The architectural design is made with the help of a tool called **Functional Decomposition**, which can be used to represent hierarchies. The architectural design has three elements :- 1) Module (represented by a box) 2) Connections (represented by arrows, connecting modules) and 3) Couple (a data element that movers from one module to another and is shown by arrow with circular tail) 	59 – 60
	2) Design of data/information flow	For designing the data/information for proposed system, the inputs required are:- a) Existing data/information flow, b) Problems with the present system and c) Objective of the new system All these have been identified in the SRA (2nd) phase and documented in SRS Report.	60
	3) Design of database	The design of database involve the following four major activities a) Conceptual Modeling, b) Data Modeling, c) Storage Structure design and d) Physical Layout design	60 – 62
	4) Design of User Interface	The points that need to be considered while designing the user interface are 1) Source documents to capture raw data, 2) Hard copy of output reports, 3) Screen layout for dedicated source-document input,	63

		4) Inquiry screens for database interrogation, 5) Graphical; and color display and 6) Requirements for special input/output device.	
	5) Physical Design	Principles for Physical Designs 1) There is tendency of developing single design and considering it the final product. However, the recommended procedure is to develop two or more alternative design and chose the best one on pre-specified criteria. 2) The design should be based upon analysis, 3) The software functions designed should be directly relevant to business activities, 4) The design should follow the standards laid down and 5) The design should be modular.	63 - 64
	6) Design of the hardware/ system software platform	In some cases, new hardware/software is required which are not available in market. The new hardware/software platform (require to support the application system) will have to be designed.	65
	- Output/Input Design	Factors to be kept in mind while designing System Output/Input:- 1) Contents (i.e. the actual pieces of data included amount the output or input source document) 2) Form (i.e. the way the content is presented to users. It may be text, graphs or diagram etc.) 3) Output/Input Volume (i.e. the amount of data/information required/entered at a time) 4) Timeliness (it refers to when user/system need output/input) 5) Media (i.e. the physical device used for input, storage or output) and 6) Format (i.e. the manner in which data are physically arranged)	66 – 71
9.	System Acquisition and Development		72
	System (Software) Acquisition	1) Acquisition Standards 2) Acquiring System Components from Vendors a) Hardware Acquisition b) Software Acquisition 3) The decision of software acquisition (buy) or software development (make) depends upon following factors:- 1) Availability of Skilled Manpower (for development of software, if not available, better to buy otherwise in-house development), 2) Cost of Programming (if more than buying cost, better to buy, otherwise, make), 3) Availability of Sophisticated Software (many time programs/software available in market are more sophisticated and required lots of customization, in such case, in-house development is better to do), 4) Timeframe available for implementation (if there is short time to implement new system, it is better to buy instead of making in-house), 5) Suitability of Software (if software available in market is not suitable to prescribed solution, in-house development is better to do), 6) Backlog of Program (In-house development takes time, if there is lots of backlog of programs awaiting development, the organization may chose to by the software) 4) Advantages of Pre-written Software 1) Rapid implementation, 2) Low Risk of failure, 3) High Quality and 4) Low Cost 5) Validation of Vendor's proposals (i.e. analysis of proposals from various vendors to select best in order to buy/acquire software) Factors to be considered while validating/evaluating Vendor's proposals:- 1) The performance capability of each proposed system in relation to its offered cost. 2) The cost and benefits of each proposal, 3) The maintainability of each proposal, 4) The compatibility of each proposed system with existing system and 5) Vendor support (benefits other than from sold software e.g. after sale support, user's training etc.) 6) Methods for Validating Vendor's Proposals 1) Check List 2) Point Scoring Analysis 3) Public Evaluation Report 4) Bench Marking Problem and 5) Test Problem	72 – 79
	Development	This step is about development of Programs required for proposed system. This explore Program Development Life Cycle (PDLC) 1) Steps in PDLC 1) Planning 2) Designing, 3) Coding, 4) Testing and 5) Operation & Maintenance 2) Characteristics of high quality program:- 1) Reliability 2) Robustness (i.e. they are robust under abnormal condition) 3) Accuracy (i.e. they perform their functions correctly and completely) 4) Efficiency (i.e. they work within spare time and with provided resources without waste) 5) Usability (i.e. they are user friendly interface enabled and easy to use) 6) Readability (i.e. they are easy to maintain) 7) They are well designed and documented.	80 – 81

	PDLC	1) Program Standards 2) Programming Language 3) Program Debugging 4) Program Testing 5) Program Documentation and 6) Program Maintenance	82 – 85
	Programming Language (Language which is used to write instruction for system)	Commonly used Programming Language:- 1) High Level General Purpose Programming Language (e.g. COBOL, C Language etc.) 2) Object Oriented Language (e.g. C++, JAVA etc.) 3) Scripting Language (e.g. JAVA Script VBS Script) 4) Decision Support or Expert System Language (PROLOG) Important criteria on the basis of which Language to be use is decided:- 1) Algorithmic Complexity, 2) Environment in which software has to be executed, 3) Performance consideration, 4) Data Structure Complexity, 5) Knowledge of Software Development staff and 6) Capability of in-house staff for maintenance.	82 – 83
	Program Debugging (It means removal of bugs from source programs.)	The activity of debugging consist of following tasks:- 1) Inputting the source program to the compiler, 2) Letting the compiler to find errors in the program, 3) Correcting lines of code that are erroneous and 4) Resubmitting the corrected source program as input to the compiler.	83 – 84
10.	System Testing	Different level of testing (also known as level of software testing):- 1) Unit Testing, 2) Integrity Testing, 3) System Testing and 4) Final Acceptance Testing	86 – 93
	1) Unit Testing	Under this form of testing individual module of software is tested one by one.	86 – 89
	- Categories of Unit Testing	1) Functional Test (to check whether program do what they are supposed to do or not) 2) Performance Test (to verify response time, execution time, memory utilization etc to evaluate performance, whether within standard or not) 3) Stress Test (testing that is used to determine the stability of program working at capacity beyond normal operational. The purpose of stress test is to determine the limitation of program) 4) Structural Test (testing concerned with examining the internal processing logic of a software system) 5) Parallel Test (under this testing common data are processed in new and old system and their outputs are compared)	
	- Benefits of Unit Testing	▪ Encourages change ▪ Simplifies Integration and ▪ Documents and Code	
	- Limitation of Unit Testing	▪ Unit testing will not identify every error in the program. ▪ Unit testing test only the functionality of the units. It does not identify integration errors. ▪ Unit testing is effective only if it is used in conjunction with other software testing activities.	
	- Types of Unit Testing	a) Static Analysis Testing (i.e. testing without executing modules) b) Dynamic Analysis Testing (i.e. testing which requires the module to be executed)	
	- Static Analysis Testing	1) Desk Check (in this SAT, programmer himself perform testing by checking logical syntax errors and deviation from coding standards.) 2) Structural Walk Through (the application developer leads other programmers thorough the text of the program and explanation.) 3) Code Inspection (the program is reviewed by a formal committee.)	
	- Dynamic Analysis Testing	1) Black Box Testing (In BBT, the internal logics of a module is not examined. Instead, test cases are designed based on the requirement specification for the module. Thereafter, test case is executed in module to determine deviation. BBT does not identify function performed which is not supposed to perform) 2) White Box Testing (In WBT, test case are designed after examining the internal logic of a module. Although, WBT reveal the internal workings of a module, it might not identify requirements what the module fails to satisfy. 3) Gray Box Testing (a combine approach of DAT which has both the features of BBT and WBT.)	
	2) Integration Testing	Under this testing individual tested modules are grouped and tested as whole. This form of testing is performed to analysis working of interfaces among modules of software.	90 – 91
	- Manner of carrying Integration Testing	1) Bottom-Up Test (In BUT, the bottom level modules are tested first. Since Higher level modules are not yet implemented, are replaced via drivers, which are dummy modules that simply confirms the interface is working.) 2) Top-Down Test (In TDT, the top level modules are tested firstly. Since bottom level modules are not yet implemented, are replaces via sub, which are dummy modules that simply confirms the interface is working correctly) 3) Hybrid Test (Hybrid Test is a combine approach of Integration Testing which has both the features. This approach is sometime called **Sandwich Testing**) and 4) Regression Integration (Under Regression Integration, instead of one time grouping, modules are grouped one by one and tested on and on)	
	3) System Testing (System Testing is a process of testing in which	The type of testing that might be carried out are as follows:- 1) **Recovery Testing** (i.e. testing of system that how well it is able to recover from crashes, hardware failure and other similar issues)	92

	software and other system elements are tested as whole, to determine whether it meets its requirement, to ensure that the new or modified system functions properly)	2) **Security Testing** (i.e. testing to determine developed system protects data and maintains functionality as intended or not) Security concept to be evaluated under this security testing are:- • Confidentiality, • Authentication, • Integrity, • Authorization, • Availability and • Non-repudiation 3) Stress or Volume Testing (i.e. testing of system beyond normal operation working) 4) Performance Testing (i.e. testing of system response time on queries and processing)	
	4) Final Acceptance Testing (FAT is conducted when the system is just ready for implementation.)	The Final Acceptance Testing has two major parts:- a) Quality Assurance Testing (to ensure that new developed system satisfies the prescribed quality standards and the development process is as per the organization's quality assurance methodology.) b) User Acceptance Testing (it ensure that the functional aspects expected by the uses have been well addressed in new system. Refer **Para 332**)	93
	- Types of User Acceptance Testing	1) Alpha Testing (i.e. the first stage testing, often performed by users within the organization) 2) Beta Testing (i.e. second stage testing, generally performed by external users.)	
11.	System Implementation or Conversion	Activities during Implementation or Changeover 1) Equipment Installation 2) Training Personnel 3) System Conversion/Changeover	94 – 98
	- Activities involved in Conversion	1) Procedural Conversion, 2) File Conversion, 3) System Conversion and 4) Scheduling Personnel and Equipment Such activities can be performed in following four ways (System Conversion/Changeover can be performed in any of the following ways/Conversion Strategies):- 1) Direct or Abrupt (sudden) Changeover (i.e. Old system immediately shut down/suspended and new system is implemented) 2) Phased Implementation (i.e. System is implemented as it developed in parts, e.g. if, 20% development is completed, the same will installed, and so on.) 3) Pilot Implementation (i.e. system is first installed in small size, for small purpose, then, if results brought are favorable, the same is implemented at large.) 4) Parallel Running Implementation (i.e. Old system is continued working vis a vis new system start working side by side.)	
12.	Post Implementation Review and System Maintenance		99 – 102
	Post Implementation Review (PIR examined the efficiency of all elements of the system to see if further improvement can be made to optimize the benefits delivered)	The purpose served a PIR to ascertain:- 1) the degree of success from the project, 2) the extent to which project meet its objectives, 3) delivered level of benefits and 4) addressed the specific requirement as originally defined The PIR is performed to meet the following objective (Objective of PIR) :- 1) Business Objectives (ensure that development performed within time and budget and producing predefined objectives.) 2) User Expectations (ensure that developed system meeting user expectations.) and 3) Technical requirement (ensure that developed system is enough flexible to meet necessary updating) During PIR, there are two basic dimensions of IS that should be evaluated:- 1) The first dimension is concerned with whether newly developed system is operation properly and 2) The other dimension is concerned with whether user is satisfied with regard to information (results/reports/output) supplied by new system. Broadly, following evaluation are made during PIR:- 1) Development Evaluation (i.e. evaluating the development process, ascertaining whether the system was developed on schedule and within budget.) 2) Operation Evaluation (i.e. Evaluating IS operation, whether Information System is capable to perform for what it is developed) 3) Information Evaluation (i.e. evaluation of information provided by developed information system.)	99 – 100
	System Maintenance The maintenance phase involves making changes to hardware, software and documentation to support its operational effectiveness and to improve system's performance; correct problems enhance security or address user requirements.	Maintenance can be categories in the following ways:- 1) Scheduled Maintenance (is anticipated and can be planned for in advance, i.e. pre-planned schedule for maintenance at regular time intervals) 2) Rescue Maintenance (refers to previously undetected mal-functions that were not anticipated and require immediate solution) 3) Corrective Maintenance (deals with fixing bugs in the code or fixing defects found) 4) Adaptive Maintenance (consist of adapting software to changes in the environment) 5) Perfective Maintenance (mainly deals with accommodating the changing user's requirements and functional enhancement to the system.) Maintenance can be undertaken under the following three categories (from Ch 3) :- 1) Corrective Maintenance (Emergency program fixes and routine debugging-logical errors.) 2) Adaptive Maintenance (Accommodations of change in the user environment.) and 3) Perfective Maintenance (User enhancement, improved documentation and recoding for improving process efficiency.)	101 – 102

13.	System Manual	- System Manual may be defined as document which contains the description of task to be performed in order to develop a system as ascertained during System Design Phase. - Contents of System Manual:- 1) General description of existing system. 2) General description of new system. 3) Files to be maintained. 4) Input responsibility. 5) Input layout 6) Output layout 7) Audit Trail 8) Macro Logics 9) Timing Estimates, 10) List of programs, 11) Glossary, 12) Controls	103
	Operation Manual	- Operation Manual may be defined as document describing the key function of a product that how it is operated and other description for users. - It is a technical communication document intended to give assistance to people using a particular system. - It is usually written by a technical writer, product or project manager or other technical staff. - Contents of Operational Manual 1) A cover page, a title page & copyright page, 2) A preface, containing details of related documents and information on how to use this manual, 3) A content page, 4) A guide on how to use function of the system 5) A troubleshooting section detailing possible errors & how to fix them, 6) A FAQs page, 7) Detail of contacts for further help, 8) A glossary and an index (in case of large manual).	104
14.	Auditors role in SDLC (also refer **Para 37**)	The audit of system under development can have three main objectives:- 1) To provide an opinion on the efficiency and effectiveness of project management, 2) To ensure the integrity of data processed and shared, 3) To access the controls being provided for the management of the system's operation.	105
15.	Auditors role in PIR	An auditor perform PIR to ensure/determine:- 1) Whether users are satisfied with the new system, 2) Whether developed system has meet the requisition as specified during SRA Phase, 3) Whether adequate controls have been employed, 4) Whether anticipated benefits have/are been achieved, 5) Whether previous system has been de-commissioned or if not so, what are the reasons thereof. 6) Which SDLC phase has not met desired objectives and whether any corrective action was taken? 7) The difference between expectation and actual results, and the reasons for the same.	105 – 106
16.	System Development Tools	Such tools which are used to develop new system (an abstract system) or improve existing system. Such tools can be grouped into four categories.	106
	Categories of SD Tools	1) System Components and Flows 2) User Interface 3) Data Attributes and Relationship and 4) Detailed System Process	107
	Some SD Tools	- Structural English (i.e. programming language used to code program to enable user to give instruction to system.) - Flow Charts - Data Flow Diagram - Decision Tree - Decision Table - CASE Tools	108
	Flow Chart	A graphical technique used to represent the input, output and processes of a business or system in a pictorial form.	108
	Data Flow Diagram (Used to illustrate the flow of data among external entities, processing activities and data storage elements.)	Elements of DFD:- 1) Data Source and Destination 2) Data Flow 3) Transformation Process and 4) Data Store	109
	Decision Table	Parts of Decision Table 1) Condition Stub 2) Action Stub 3) Condition Entries 4) Action Entries	110
	Decision Table	Four parts of Decision Table 1) Condition Stub 2) Action Stub 3) Condition Entries 4) Action Entries	110
	CASE Tools	Set of tools that an ideal CASE tool should have:- - Data Dictionary - Computed aided diagramming tools - Word processing - Screen and report generator - Prototyping - Project Management - Code Generation and - Reverse Engineering	111
	Data Dictionary	Data dictionary is a computer file that contains descriptive information about the data items in the files of a business Information System. Thus Data Dictionary is a computer file about data in that computer.	112 – 113

		Benefits of Data Dictionary to System Auditor 1) A data dictionary can help to establish an audit trail, because it can identify the input source of data items, the computer programs that modify it and the managerial reports on which the data items are output. 2) A data dictionary can also used to plan the flow of transaction data through the system.		
17.	System Development Approaches	1) Waterfall/Traditional 2) Prototype 3) Incremental 4) Spiral 5) Rapid Application Development (RAD) 6) Agile Methodologies	Basis for explanation:- - Framework - Basic Principle - Strength and - Weakness - Diagram	114 – 123

	Chapter – 5	**Risk Assessment Methodology and Application**			126 – 156
1.	Risk Assessment (also refer **Para 144**) Risk assessment is a critical step in Disaster and Business Continuity Planning. Purpose of Risk Assessment and analysis involves threat identification and risk mitigation.	Risk Assessment is a process used to identify the risk factors and then analyze and evaluate the identified risk factors to develop an appropriate risk mitigation plan. Risk Assessment seek to identify:- 1) Which business purposes and related resources are critical to the business, 2) What threats or exposures exist that can cause an unexpected interruption of business processes, 3) What cost accrues due to an interruption? Risk Assessment consist of two basic components, namely:- - Data Collection and - Analysis of data collected			126, 133
	- Areas to be focused upon during Risk Assessment:-	1) Prioritization (all critical assets are identified and inventoried), 2) Indentifying Critical Application, 3) Assessing their impact upon Organization, 4) Determining recovery time frame, 5) Assess insurance coverage, 6) Identification of exposures and implication and 7) Development of Recovery Plan			
	Risk Analysis	Consideration in Risk Analysis includes:- 1) Investigating the frequency of occurrence of particular threat, 2) Determination of degree of predictability of disaster/threat, 3) Analyzing speed of onset of the disaster, 4) Determine the amount of forewarning associated with threat, 5) Identify the consequences of a threat 6) Considering the impact of a threat and 7) Determining the existing and required redundancy level.			134
	- Risk	A risk is the likelihood that an organization would face a vulnerability being exploited or a threat becoming harmful. (Types of Risk, refer **Para 283**)			127 – 128
	- Threats	Threat A threat is an action, event or condition where there is a compromise in the system; system's quality and ability to inflict (impose) harm to the organization. Harm to IS can be in following form:- ▪ Destruction ▪ Disclosure ▪ Adverse modification of data and ▪ Denial of service			127 – 128
	- Vulnerability	It is the weakness in the system safeguard that expose the system to threats. Vulnerability may be weakness in an information system, cryptographic system (i.e. security system) or other component (e.g. system security procedure, hardware design, internal control) that could be exploited by a threat.			127 – 128
	- Exposure	An exposure is the extent of loss the organization has to dace when a risk materializes.			127 – 128
2.	Threats to the Computerized Environment	1) Power failure 2) Communication failure 3) Errors 4) Disgruntled employees 5) Malicious codes	6) Natural Disaster 7) Theft or destruction of Computer resources 8) Abuse of Access Privilege by Employees 9) Downtime due to technology failure 10) Fire etc.		129 – 130
	Controls suggested by System Auditors against various threats to computer systems and resources. (**Ch – 6, Point 6, Para 184**)				
3.	Threats due to Cyber Crimes	1) Embezzlement 2) Fraud 3) Theft of Proprietary Information	4) Denial of Services 5) Computer Virus		
4.	Risk Classification	Systematic Risk and Unsystematic Risk			137 – 138
		Basis for difference	Systematic Risk	Unsystematic Risk	
		- Meaning	Risk which are unavoidable and common for all organization. E.g. Natural Disaster.	Risk which are avoidable and unique to particular organization. E.g. theft, fire.	
		- Avoidable	Such risk are unavoidable	Such risk can be avoided with proper management.	
		- Mitigation	Such risk can be mitigated through management control process and does not involve technological solution	Such risk can be mitigated only through advance technological or systematic solution.	
5.	Risk Management Risk Management aims to identify, select & implement the controls that are necessary to reduce residual exposures to acceptable level. (**Para 147**)	Risk management is a process which involve following steps:- 1) Identification of Information Assets, 2) Valuation of Information Assets, 3) Indentifying the potential threats, 4) Information Risk Assessment and 5) Developing strategies for Information Risk Management			135
	1) Identification of Information Assets	Identified assets can be grouped as below:- A. Logical Assets - Data/Information (master files, transaction files, archival files) and Software (System and Application – compilers, utilizes, DB Management System etc.) B. Physical Assets 1) Hardware (Mainframe, Mini, Micros, Peripherals and Storage Media) 2) Personnel (End users, programmers, operators etc.) 3) Documentation (System and Program Documentation, DB Documentation, Insurance Policies, Contracts/agreement etc.) 4) Supplies (Negotiable Instrument, paper, tapes etc.) and			139

		5) Facilities (furniture, office space, computer room, tape storage racks etc.)	
	2) Valuation of Information Assets	Factors affects the value of an Information System Asset/resource:- 1) Who values (the asset will have more value for its user than others) 2) How lost (assets which may lost due to accident, will have less concentration than assets which might lost due to irregularities or careless behavior) 3) Asset age (more older the asset will have less value) 4) Loss period and 5) Sensitivity	140 – 141
	Techniques for valuation of Assets	- Logarithmic Value - Judgment and Intuitions - Delphi Technique - Scoring Approach - Quantitative Approach and - Qualitative Approach	
	3) Identifying Potential Threats (also refer "various threats to Organization at **Para 129**)	Threats could affect the :- - Confidentiality (Confidentiality involves the protection of resources from disclosure to unauthorized person and processes) - Integrity (Integrity requires that the business information and related process should not suffer any intentional or accidental unauthorized modification which may result in serious consequences to the business) and - Availability (Availability relates to whether the information and information technology processes are available to the authorized business users when required.)	143 – 144
	4) Information Risk Assessment (also refer **Para 126 & 133**)	This step covers following three steps:- 1) Vulnerability Analysis, 2) Probability Assessment and 3) Impact Analysis	144 – 145
	5) Developing Strategies for Information Risk Management	The strategies to manage risk may fall into one or more of the following categories (types of Risk Management Strategies):- 1) Risk Avoidance Strategies 2) Risk Mitigation Strategies 3) Risk Transfer Strategies and 4) Risk Retention/Acceptance Strategies	145 – 147
6.	Risk Management Cycle	RM Cycle is a process involving following activities:- - Identify the Risk Area, - Assess the Risk, - Develop risk management plan, - Implement Risk & Management actions and - Re-evaluation of Risk	147
	Steps in Risk Management Cycle	1) Risk Identification, 2) Risk Evaluation & Ranking 3) Risk Assessment and 4) Risk Mitigation	
	1) Risk Identification	This step covers identification of such threats and associated risk which can affect vulnerability of the business and information system. Asking following questions help to identify potential risk to critical business and information system resources:- - What could go wrong? - How could we fail? - Where are we vulnerable? - How could someone steal from the department? - What is our greatest legal exposure? ..etc.	148
	2) Risk Evaluation & ranking	This step involve evaluation of identified risk, their classification on some scientific basis (such as on the basis of their expected exposures). Risk Evaluation Techniques:- 1) Judgment and Intuition, 2) Delphi Approach 3) Scoring 4) Quantitative Approach and 5) Qualitative Approach	148 – 152
	3) Risk Assessment	**Refer Para 123, 133 & 144**	153
	4) Risk Mitigation	Under this step, various risk mitigating techniques are identified and most appropriate technique is selected. Most common Risk Mitigation Techniques/tools are:- 1) Insurance (also refer **Para 181**) 2) Outsourcing and 3) Service Level Agreement Before adopting any risk mitigating tool, do proper cost-benefit analysis.	155 – 156

	Chapter – 6	**Business Continuity Planning and Disaster Recovery Planning**	157 – 191
1.	Business Continuity Planning	BCP is guiding documents that allow/enable the management team to continue operations, running the business under stressful and time compressed situation. The plan layout the various steps to be initiated on occurrence of a disaster, to combating it and returning to normal operation. BCP covers the following:- 1) Business resumption planning (the operation's piece of BCP), 2) Disaster recovery planning (the technological aspect) and 3) Crisis Management.	158 – 159
		BCP = Business Resumption Planning, Crisis Management and Disaster Recovery Planning (DRP) (**Para 173**) DRP = Emergency Plan, Back-up Plan, Recovery Plan and Test Plan	
	Business Continuity Life Cycle	BCLC is broken down into four broad & sequential section:- 1) Risk Assessment 2) Determination of recovery alternatives 3) Implementation of recovery plan and 4) Recovery plan validation	
	Objectives of BCP	BCP should be to 1) Provide for the safety and well-being of peoples at the time of disaster (i.e. peoples protection during disaster) 2) Continue critical business operations 3) Minimize the duration of a serious disruption to operations & resources, 4) Minimize immediate damage and loss, 5) Facilitate effective co-ordination of recovery task 6) Reduce the complexity of the recovery efforts and 7) Identify critical lines of business and supporting functions.	160
	Goals of BCP	1) Identify weaknesses and implement a disaster prevention program, 2) Minimize the duration of a serious disruption to business operation 3) Facilitate effective co-operation of recovery task and 4) Reduce the complexity of the recovery efforts.	160
2.	Methodology for developing BCP (similar to SDLC)	The methodology for developing BCP emphasizes on the following:- 1) Providing management with a comprehensive understanding of the total efforts required to develop and maintain an effective recovery plan. 2) Obtaining commitment from appropriate management to support & participate in the effort, 3) Defining recovery requirement from the perspective of business functions, 4) Documenting the impact of an extended loss to operation and key business functions, 5) Focusing appropriately on disaster prevention and impact minimization as well as orderly recovery, 6) Selective business continuity teams that ensure the proper balance required for plan development 7) Developing a business continuity plan that is understandable, easy to use and maintain & 8) Defining how business continuity consideration must be integrated into ongoing business planning and system development processes in order that the plan remains viable over time.	161 – 162
	Phases in BCP Methodology	1) Pre-planning, 5) Plan development, 2) Vulnerability Assessment 6) Testing programs, 3) Business Impact analysis, 7) Maintenance Program/Plan and 4) Detailed definition of requirements, 8) Plan Implementation A BCP/DRP can never be implemented without happening of unwanted event and therefore, it requires regular maintenance to keep it operative and Plan Implementation Phase comes after maintenance.	162
	1) Pre-planning	In this phase, plan developer obtains an understanding of the existing and projected system environment of the organization. The two key deliverables of this phase are:- 1) The development of a policy to support the recovery program and 2) An awareness program to educate management and senior individuals who will be required to participate in the business continuity program.	162 – 163
	2) Vulnerability Assessment	This phase addresses measures to reduce the probability of occurrence of a threat. This phase will involve following tasks:- 1) A thorough security assessment of the system and communication environment including other assets, 2) Present/submit findings with recommendation resulting from the activities of the security assessment to the Steering Committee, so that corrective action can be initiated in a timely manner. 3) Define the scope of planning efforts, 4) Develop a Plan Framework, 5) Analysis, recommend and purchase "recovery planning end maintenance software" required to support the development and maintenance of the BCP and 6) Assemble BCP team and conduct awareness session.	163 – 164
	3) Business Impact Analysis BIA is a means of assessing the potential impacts resulting from various events or incidents. The purpose of BIA is to understand the degree of potential loss and various other unwanted effects which could occur on metallization of a threat.	The following tasks are undertaken in this phase:- 1) Identify Organizational Risk (refer, Risk identification at **Para 148**) 2) Identify Critical Business processes, 3) Identify and quantify threats/risk to critical business processes, 4) Identify dependencies and interdependencies of critical business processes, 5) Determine the maximum allowable downtime, 6) Identify the type and quantity of resources required for recovery and 7) Determination of impact to the organization in the event of a disaster. Ways to obtain such information (also refer fact finding techniques at **Para 50**):- 1) Questionnaires, 2) Interviews,	165 – 166

		3) Examination of documents and 4) Workshop	
	4) Detailed definition of requirements	During this phase, a profile/list of requirements for recovery is made. This profile/list should include:- 1) Hardware (mainframe, communication devices etc.) 2) Software (vendor supplied or in-house developed) 3) Documentation (user, procedure etc.) Another key deliverable of this phase is the definition of the plan scope, objectives and assumption.	166
	5) Plan Development	In this phase, recovery plans components are defined and plans are documented. This phase also involves:- 1) Te implementation of changes to user procedures, 2) Upgrading of existing data processing operating procedures and 3) Definition of recovery teams, their roles and responsibilities. The objective of this phase is to determine the available options and formulation of appropriate alternative operating strategy to provide timely recovery for all critical processes and their dependencies.	167
	6) Testing of Plan	Testing of Plan and Test Plan are same except that "Testing of Plan" is considered as a Phase of BCP Methodology while "Test Plan" is a type/part of DRP. The objective of performing testing of developed DRP is to ensure that:- 1) The recovery procedures are complete and workable, 2) The success or failure of the business continuity training program is monitored, 3) The resources are obtainable and operational to perform recovery processes, 4) The competence of personnel in their performance of recovery procedures can be evaluated and 5) The manual recovery procedures and IT backup system are current and can either be operational or restored.	168
	7) Maintenance Program	Maintenance of the plan is critical to the success of actual recovery. The tasks undertaken in this phase are:- 1) Defining the ownership of responsibility for maintaining the various BCP/DRP strategies, 2) Identifying the BCP/DRP maintenance triggers to ensure that any organizational, operational and structural changes are communicated to the personnel who are accountable for ensuring the plan remains up-to date. 3) Determine the maintenance regime to ensure the plan remains up-to date, 4) Determine the maintenance processes to up-to date the plan and 5) Implement "version control procedures" to ensure that the plan is maintained up-to date.	169
	8) Testing and Implementation	Here, testing implies testing of plan which is ready to face any disaster, at regular interval to keep it up-to date, effective and efficient. Specific activities of this phase include the following:- 1) Defining the test purpose/approach, 2) Identifying test teams, 3) Structuring the test, 4) Conducting the test, 5) Analyzing test results and 6) Modifying the plan, as appropriate.	170
3.	Types of DRP Plans	1) Emergency Plan (states about the activities to be undertaken immediately after disaster) 2) Backup-plan (states about the pre-disaster activities in respect of various backup plans, options and devices, where to kept them) 3) Recovery Plan (states about the post disaster activities) and 4) Test Plan (states about the testing of above three plans- refer **Para 171**)	
	1) Emergency Plan	The emergency plan specifies the actions to undertaken immediately when a disaster occurs. During making/developing emergency plan, following aspects must be considered:- 1) Who is to be informed immediately on occurrence of disaster, 2) Actions to be undertaken immediately, 3) Any evacuation procedure (exit plan), 4) Return procedure (i.e. conditions that must be met before the site is considered safe).	173
	2) Back-up Plan The back-up plan is intended to restore operations quickly so the information system function can continue to service an organization. The most difficult part in preparing a back-up plan is to ensure that all critical resources are backed-up.	The back-up plan specifies:- 1) The type of back-up to be kept, 2) Frequency with which back-up is to be undertaken, 3) Procedures for making back-up, 4) Location of back-up resources, 5) Site where these resources can be assembled and operations re-started, 6) Personnel who are responsible for gathering back-up resources and restarting operations, 7) Priorities to be assigned/followed to various recovering systems/resources and 8) Timeframe for recovery of each system/resource. The following resources must be considered:- A. Logical (Data/Information and Software – System & Application) B. Physical (Personnel, Hardware, Documentation, Facilities and Supplies)	176 – 180
	- Types of Back-up Plan:-	1) Full back-up (In full back-up, entire data is selected for copy in compressed form with password protection. It takes much time to complete and also requires more storage space. That's why it is not opted much time to avoid such delay.) 2) Mirror back-up (It is similar to Full Back-up except that there is not compression of data backed-up and not password protection. Under this back-up, exact copy of original data is made within short period.) 3) Incremental Back-up (under this back-up, after last back-up, only changed and modified data/files	

		are back-up. An **incremental backup** preserves data by not creating multiple copies that are based on the differences in those data: a successive copy of the data contains only that portion which has changed since the preceding copy has been created.) 4) Differential Back-up (under this back-up, after a full back-up, only changes files/data are backed-up).	
	- Back-up tips:-	1) Draw a simple, easy to understand plan, 2) Be original; keep a record of "what was backed-up, when backed-up" etc. 3) Utilize the "*volume shadow copy service*" in Window Server 2003, 4) Always check option to verify backed-up data, 5) Create a reference point where you know everything is working properly, 6) Check the option to restrict restoration of data only to Administrator and 7) Create a step-by-step guideline for restoration of data.	
	- Back-up media:-	While selecting back-up media, following factors must be considered:- 1) Speed (higher the speed, lesser time to complete back-up), 2) Capacity (more the capacity/space, more data will be backed-up), 3) Cost (should be lesser than value of data to be backed-up), 4) Reliability and 5) Extensibility	
	- Back-up Options (i.e. location where back up storage/arrangement made available):-	1) Cold Site (only critical assets are stored off-site), 2) Hot Site (all assets are stored outside), 3) Warm Site (a intermediate approach) and 4) Reciprocal Agreement (an agreement with other organization to share their sites in case of disaster in other sites for a pre-determined period. **Also refer Para. 191**)	
	3) Recovery Plan	1) Recovery plan set out procedures to restore full information system capability after disaster from back-up site. 2) Recovery plan should identify a recovery committee that will be responsible for working out the specifics of the recovery to be undertaken. 3) The plan should specify the responsibilities of the committee and provide guidelines of priorities to be followed. 4) The plan might also indicate which application is to be recovered first.	174
	- Contents of DRP (disaster recovery procedural plan):-	1) The conditions for activating the plans (which describe the events/activities on happening of which, plan must be initiated), 2) Emergency Procedure (which describe the action to be taken immediately on happening of disaster), 3) Fallback procedure (which describe the actions to be taken to move essential business activities or support services to an alternative temporary location), 4) Resumption procedure (which describe the action to be undertaken to return to normal position), 5) Emergency Phone List, 6) Name of employees trained for emergency situation, 7) Checklist of Inventories, 8) Medical Procedure to be followed in case of injury, 9) Insurance papers and claims forms, 10) A maintenance schedules, 11) Awareness and education activities, 12) List of vendors. …etc. Such contents are classified into types of Plan (**Para 173**)	175
	4) Test Plan	The purpose of test plan is to identify deficiencies in the emergency, back-up and recovery plans. Testing Methodology and Checklist (Types of Test Plan):- 1) Hypothetical Testing (it is a theoretical test and does not involve physical/active testing) 2) Component Test (component is a smallest set of instruction within the DRP, testing of which called component testing.) 3) Module Test (module is a combination of components, testing of which called module testing) 4) Full Test (it covers testing of modules made with different components.) Objective of Full Testing:- (1) Confirm that the total time elapsed meets the recovery time objective and (2) Prove the efficiency of the recovery plan, to ensure a smooth flow from module to module. Objective of Testing – refer **Para 168**	170 – 173
4.	Insurance (also refer **Para 155**)	Insurance is one of key method for risk mitigation. Under insurance scheme, the risk of loss from unexpected event transferred to other person, i.e. it is a risk avoidance strategy.	181 – 182
	Kind of insurance:-	1) First Party Insurance (It's an insurance scheme, in which the policy holder lodge claim against damage/loss to himself.) 2) Third Party Insurance (It's an insurance scheme, in which the policy holder lodge claim against damage/loss to a third party.)	
5.	Auditors' role in BCP	Audit tools & techniques used by a System Auditor to ensure efficiency and effectiveness of DRP:- 1) Automated Tools 2) Internal Control Auditing 3) Disaster or Security Checklist and 4) Penetration Testing	183 – 184
6.	Suggested **Control Measures** against various threats, risk & exposure to Computer System to be verified by System Auditor	Threat, Risk & Exposure / Suggested Control Measures Common Controls for:- / - Implementation of security policies, procedures & standards, - Use of encryption techniques & digital signatures, Lack of Integrity / - Security awareness program, Lack of Confidentiality / - Training of employees, Lack of System Availability / - Installation of audit trails,	184 – 187

		- Use of password and other authentication techniques, - Update anti-virus software,	
		1) Lack of Integrity - Division of job, - Implementation of user identification, authentication & access control technique, - Back-up of system & data, - Audit of adequacy of data integrity	
		2) Lack of Confidentiality - Require employees to sign a "non-disclosure undertaking" - Implementation of physical and logical access controls, - Secure storage of important media and data files, - Audit of confidentiality of data 3) Disgruntled Employees - Implementation of physical and logical access controls, - Logging and unsuccessful logins notification, - Protection of modem & network devices, - Security awareness program, - Training of employees, - Job enrichment and job rotation	
		4) Lack of System Availability - Implementation of software configuration controls, - Insurance coverage, - Back-up power supply, - Audit of adequacy of availability safeguards 5) Hackers & Computer Crimes - Install firewall and intrusion detection systems, - Change of system passwords frequently, - Use of encryption techniques while storing and transmitting data, - Use of digital signature	
		6) Unauthorized Users - Use of password and other authentication techniques, - Implementation of physical and logical access controls, - Regular audit program 7) Terrorism & Industrial Espionage - Use of traffic padding and flooding techniques to confuse intruders, - Use of encryption during program & data storage and transmission. - Use of network configuration controls, - Installation of intrusion detection program.	
7.	Single Point of Failure (SPOF)	A SPOF is a part of a system that, if it fails, will stop the entire system from working. Single point of failure have increased significantly due to the continued growth in the complexity in the organization's IS environment. This growth has occurred due to change in technology and customer's demand for new channels in the delivery of service and/or product, e.g. e-commerce.	187 – 188
	SPOF Analysis	An analysis which is performed with objective to identify any such single point of failure within the organization's infrastructure, in particular the information technology infrastructure.	187
8.	Technology Risk Assessment	To ensure that all single points of failure are identified, it is essential to perform Technology Risk Assessment. The technology risk assessment needs to be a mandatory requirement for all projects to ensure that proactive management of risks occurs and that no single point of failure is inadvertently built into the overall architecture.	188 – 189
	Objective of TRA (also refer Objective of Risk Assessment at **Para 126, 133 & 144**):-	1) Identify information technology risk, 2) Determine the level of risk, 3) Identify the risk factors, 4) Develop risk mitigation strategies	
	Benefits of performing TRA	1) It is a business-driven process to identify, quantify and manage risks while detailing future suggestion for improvement in technical delivery, 2) It is a framework that governs technical choice and delivery processes with cyclic checkpoints during the project lifecycle. 3) It helps in interpretation and communication of potential risk impact and where appropriate, risk reduction to a perceived acceptable level. 4) It helps in implementation of strict disciplines for active risk management during the project lifecycle.	
9.	Reciprocal Agreement	It is a one of Back-up option under which two or more organization makes an agreement among them to share their sites in case of happening of disaster in other premises for a pre-determined period.	191
	Factors to be considered while drafting Reciprocal Agreement	1) How soon the site will be made available to organization after disaster? 2) The number of organizations who will be there to share same site. 3) The period for which site can be use. 4) The conditions subject to which site can be use. 5) The other facilities and services that site owner will provide. 6) What control will be in place?	

	Chapter – 7	**An overview of Enterprise Resource Planning**	192 - 215
1.	ERP Definition	An ERP System is a fully integrated business management system covering functional areas of an enterprise, to make optimum use of resources. ERP promises one database, one application and one user interface for the entire enterprises.	192
2.	ERP's Objectives (as provided in Chapter 2)	1) Provide support for adopting best business practice, 2) Implement best business practice to enhance productivity, 3) Empower the customers and suppliers to modify the implemented business processes to suit their needs.	192
3.	Characteristics of ERP (characteristics means something which a system should have to qualify being called ERP)	1) Integrated (the system should be a integrated of all functional areas & resources) 2) Flexible (the IS should be enough flexible to respond changing needs and environment) 3) Modular and Open (the IS should be open and modular to adopt and remove any existing or new module, if required) 4) Comprehensive (the system should be able to support variety of functions and activities) 5) Beyond the Organization (the system should work and linked beyond the organization to customers, suppliers and banks) 6) Best Business Practice (the system should be such which represent best business practices in the industry)	193
4.	Features of ERP (features means what an ERP system have in addition to what traditional IS do not have)	1) ERP provides multi platform, multi facilities, multi mode manufacturing, multi currency, multi language with common interface. 2) ERP facilitates companywide Integrated IS covering all functional aspects, 3) ERP provides integration beyond the organization, 4) ERP bridge the information gap between organizational units, 5) ERP is the solution for better project management, 6) ERP allows automatic introduction of latest technology, 7) EPR eliminates most business problems shortly, 8) ERP provides **intelligent business tools like DSS, EIS,** Data Mining etc.	194
5.	Why Companies undertake ERP? Because (May 2010)	What factors would be considered before undertaking implementation of an ERP system? 1) Integrated Financial Information, 2) Integrated Customer Order Information, 3) Standardize & Speed up Manufacturing Processes, 4) Standardize HR Information and 5) Reduce Inventory	195
6.	Benefits of ERP	1) Better use of Organizational Resources 2) Lower Operation Cost, 3) Pro-active Decision Making, 4) Decentralized Decision Making, 5) Enhanced Customer Satisfaction and, 6) Flexibility in Business Operation	196 – 197
7.	Limitation of ERP	Though ERP has many benefits, it has some limitations which are as below:- 1) ERP provides current status only. 2) The methods used in the ERP application are not integrated with other organizational or divisional system (i.e. the methods of ERP are not integrated with other methods of other IS).	197
8.	Risk and Governance Issues with ERP	In addition to above discussed risk to computerized IS, following are certain risk associated with ERP:- 1) Single Point of Failure (since ERP is a integrated system, there is always risk of single point of failure due to some critical single points), 2) Job-role Change (ERP requires change in jobs, which is also a risk upon employees performance reduction) 3) Online-real time (ERP is a online-real time system, which have some network associated risk) 4) Change Management (ERP Implementation required complete change from existing situation, and thus requires proper change management), 5) Broad System Access (since ERP works beyond the organization and thus always have risk of unauthorized access and other risk), 6) Dependency on External Assistance (the operation of ERP are indeed performed by internal users, however, its maintenance is within some outside experts which makes organization dependency upon outsider, the absence of whom may lead some problem) 7) Program Interface and Data Conversions, 8) Audit Expertise, 9) Structural Change and 10) Distributed Computing Experience Some risk which are associated with ERP due to its link with E-commerce:- 11) Single Sign-in 12) Data Content Quality and 13) Privacy and Confidentiality Issue	198
9.	Reasons of failure to achieve ERP Implementation Objectives	The reason are similar to "Reasons to failure to achieve SD Objectives" as explained at **Para 35**. However here (as given in Study Material) are some associated with ERP:- 1) Peoples/users resistant to change and 2) Customizations (makes the software more unstable and harder to maintain)	199
10.	ERP Implementation Methodology	The ERP Implementation Methodology is much similar to SDLC Methodology. However, SDLCM is a broad concept and ERPIM is limited to ERP only, which comprised steps explain as below:- 1) Identify the need for Implementation of ERP package, 2) Evaluate the "as is" situation of the business (i.e. understand existing system), 3) Deciding the "would be" situation (i.e. defining requirements/objectives of ERP), 4) Re-engineering of the business processes, 5) Evaluating various available ERP Packages, 6) Selecting the most suitable ERP package for implementation, 7) Installing the required hardware and networks for the selected ERP Package, 8) Selection/Establishment of Implementation Consultants Teem for assistance in implementation & 9) Implementation of ERP Package.	199
11.	Business Process Re-engineering (BPR)	BPR is 4th step in ERP Implementation Methodology. It means fundamental rethinking & radical redesign of processes to achieve dramatic improvement. Here dramatic improvement means improvement more	200 – 201

		than 80%. Every organization intends to implement ERP has to reengineer its processes in one form or the other.	
	Why BPR is required..?	When an enterprise does not have optimized business processes, ERP implementation needs a process re-engineering which enable to capture knowledge of thee experts into the system, thereby gaining considerable benefits in the productivity.	
	Objective of BPR:-	1) Reduce business process cycle time (by eliminating unnecessary processes/steps), 2) Reduce the number of decision points to a minimum level and 3) Streamlining the flow of information and eliminating the unwanted information flow.	
	Principles/Rules of BPR:-	1) Single point responsibility for any process (i.e. one person should be responsible for one task), 2) Continuous communication and co-ordination between person jointly responsible for a task & 3) Common database	
12.	Business Engineering (BE) It means BPR with application of Information Technology. BE is the re-thinking of business processes to improve speed, quality and output of the product or service.	BE is the method of development of business processes according to changing needs. Features of BE:- 1) It involve application of Information Technology, 2) Emphasis on the concept of Process Oriented Business Solution enhanced by the client server computing in Information Technology, 3) Efficient redesign of company's value added chain is main concern and 4) It is a method of development of business processes according to changing needs.	201 – 202
13.	Factors to be consider while evaluating Various ERP Packages	While evaluating various ERP Packages in the market, the management should check all such characteristics that a system must have to be called ERP (as explained at **Para 193 and 203**). In addition to such characteristics following factors should also be checked:- 1) Cost and Benefits Analysis, 2) Local or Global Presence, 3) Life of the Package, 4) Implementation Cost 5) Customization required or not etc.	203 – 204
14.	Challenges involved in ERP Implementation	1) Lack of Proper Coordination, 2) Undefined Roles and Responsibilities, 3) Lack of Complete Package,, 4) Lack of Support, 5) Objective Recognition, 6) Acceptance of new process, 7) Lack of defining the methodology, 8) Non-availability of expert consultants, 9) Preparation of Guidelines and 10) Monitoring Limitation	205
15.	Post Implementation Task	Following are certain tasks (as provided in study material) which have to be performed to suit the future ERP Environment:- 1) Develop new job descriptions and organization structure. 2) Determine the skill gap between existing jobs and envisioned jobs, 3) Access training requirements and if required develop and implement training program, 4) Develop and amend HR, Financial and Operational Policies and 5) Develop a plan for workforce logistics adjustments.	207 – 208
16.	Implementation of CSF and KPI		208
17.	Key Planning and Implementation Decisions	1) ERP or Not a ERP, 2) Follow Software's Processes or Customized, 3) In-house or Outsource and 4) Big Bang or Phased Implementation	209
	ERP or Not a ERP	This consideration made organization to evaluate whether they needed for integrated system or the existing system is well enough for them. For a small organization having no or few units at different geographical place will not require such integrated system, while, on the other hand, an organization having many units at various location will require such integrated system to make available true picture of progress at real time update.	209
	Follow Software's Processes or Customized	Under this consideration, the organization has to take decision about type of software. Should they go for pre-defined package or should order for customized software. In this first case, i.e. pre-defined software, the organization has to perform re-structuring of organizational processes to make them in accordance of software's processes, while in second case, i.e. customized software, they will not require to perform change in existing processes (except some few changes). This will involve consideration upon cost of re-structuring and cost of customization, i.e. proper cost analyze has to perform.	209 – 210
	In-house or Outsource	Under this consideration the organization has to decide whether establish in-house team of expert for Implementation of ERP or should outsource the implementation work. Generally, outsourcing provides more advantage and makes organization to keep concentrating on their core business activities, they go for outsourcing.	210 – 211
	Big-Bang or Phased Implementation	This is consideration about Implementation Strategy (refer **Para 94** for various implementation strategies). Big-bang strategy advocates onetime implementation of entire system at all units of the organization, while Phased Implementation explains implementation of system at some units firstly, then its expansion.	210 - 211
18.	ERP Implementation Guidelines	The general guidelines to be following before starting the implementation are:- 1) Define the needs and organization culture to adopt a suitable matching implementation technique, 2) Re-design the business processes prior to starting the implementation, 3) Establish a good communication network across the organization, 4) Provide a strong and effective leadership to motivate the people down the line, 5) Find an effective and efficient Project Manager, 6) Create a balanced team of Implementation Consultants and Users, who can work together, 7) Select a good implementation methodology with minimum customization, 8) Adopt the new system & make required changes in the working environment to use the system effectively.	212
19.	How to get over the barriers on successful implementation of	The success of ERP implementation mainly depends upon how closely the implementation consultant users and vendors work together to achieve the overall objective of the organization.	

	ERP. (May 2010) Also refer "Key Planning and Implementation Decisions" at **Para 209**	One can get over the impediments for successful implementation of ERP in the following ways:- 1) Appropriate Coordination, 2) Appropriate selection of ERP Software, 3) Standardization of Business Process and 4) Proper compatibility between man and method.	
20.	Reasons which requires course correction many times during post implementation. (Nov 2010)	During post implementation there will be need for course correction many times. It may be because of the following reasons:- 1) Change in business Environment (which requires change in the CFSs) 2) Review Results (indicates a need for change in some processes) 3) Change in Vision of ERP. 4) Change in Hardware and Communication Technology and 5) New additions to the business (which requires extra functionality).	213
21.	Various ERP Packages	SAP, Oracle, Baan, Business Planning and Control System, System 21 etc.	

	Chapter – 10	**Information Technology (Amendment) Act, 2008**	216 - 253
1.	Objective of the Act	1) Grant legal recognition to E-commerce, 2) Give legal recognition to Digital Signature, 3) Facilitate E-filling with Govt. agencies, 4) Facilitate electronic storage and maintenance of records 5) Give legal recognition to keeping books of accounts in e-form by banking companies, 6) Amend the Indian Penal Code, the Indian Evidence Act, the Banker's Book Evidence Act and the RBI Act.	216
2.	Application of Act	The act is extended to the whole of India.	217
	Applicability Outside India	According to Section 75, the act shall also apply to any offence or contravention under the act, the rules, the regulations or order there under committed outside India by any person irrespective of his nationality, **if such offence or contravention related t or affects any computer, computer system or computer network in India.**	243
	Non Applicability of the Act	1) Negotiable Instrument (except cheque), 2) Power of Attorney, Conveyance Deed or Will and 3) Trust Deed	217
3.	Adjudicating Officer	AO means officer appointed u/s 46(1). Sec 46 provides Power to Adjudicate. For this purpose, the central govt. appoints an officer called Adjudicating Officer.	217- 218
	Functions of Adjudicating Officer	Adjudicating Officer adjudicates any person who has committed any contravention or offence under the act, rules regulations or order there under which rendered him to pay penalty or compensation. A matter (where any person has been affected by an offence under this act, or any person has contravene the provision of this act) lies before AO for the first time. He then proceeds with SCN to accused party and wait for reply. Thereafter, either after proceedings or ex-party, the AO may impose such penalty or grant such compensation to affected party, as he think fit according to act. AO can deal with matters which involve claim for damage not exceeding Rs. 5 Cr. Where the claim exceeds Rs. 5 cr., the matter shall be handled by the competent court. While determining penalty or compensation amount, AO has to consider certain factors (Sec 47). 1) The amount of gain to accused person, 2) The amount of loss of aggrieved party and 3) The repetitive nature of the default/offence/contravention. It is provided u/s 77 that, there may be award of compensation or penalty under any other law irrespective that the fact that the same has been considered under this act. (**Para 243**)	217 – 218
	Powers of Adjudicating Officer	1) Every AO has the power of Civil Court, some of which are as below:- 2) Summon any person (i.e. cause any person to present in person or through representative before him) , 3) Enforce any person to take oath, 4) Receive evidence on affidavit, 5) Issue commission for examination of witnesses or documents, 6) Review his decision, 7) Dismissing an application for default or deciding it ex-party, 8) Any other matter, which may be prescribed.	217 – 218
4.	Appropriate Government	Means State government where the matter related to - any state law enacted under List III of the 7th Schedule to the Constitution (concurrent list) or - matter enumerated in the List II of the 7th Schedule to the Constitution (state list) Central Government for any other matter.	218 – 219
5.	Certifying Authority Means a person who has been granted a license (to issue e-signature certificates u/s 35) u/s 24.	Section 21 provides that any person can make an application to act as Certifying Authority. Section 22 provides the form for and procedure of application filling. The application form shall be in such form as may be prescribed by CG. Such form shall be accompanied by 1) A statement of practice 2) A statement for identification of applicant, 3) Payment of fee as may be prescribed by CG (shall never exceed Rs. 25,000), 4) Such other documents as may be prescribed by the CG. U/s 24 the Controller may grant license to issue Electronic Signature Certificates or reject the application after giving reasonable opportunity for representing his case. The validity of license issued under this section shall be such as may be prescribed by CG. U/s 23, the Certifying authority has option to apply for renewal of license. However, such option can be exercise only during 45 days before the expiry of validity of license. U/s 25, the Controller has power to revoke or suspend license under certain circumstances. (refer **Para 221**)	219 - 222
	Revocation or suspension of license granted u/s 24 (Power of Controller) Sec 25	**Revocation of License granted u/s 24 [Sec 25(1)]** The controller may revoke any license granted u/s 24, if he think fit, after making such enquiry that Certifying Authority (i.e. license holder) has ▪ Made incorrect statement (for fresh application for license or for renewal of license), ▪ Failed to comply with terms & conditions subject to which license was granted, ▪ Contravene any provision of this act rule, regulation or order thereunder, or ▪ Failed to maintained standards specified u/s 30 of the act. **Suspension (can be made for maximum 10 days) [Sec 25(2)]** The controller may suspend such license, if he has reasonable cause to believe that there is any ground	221

		for revoking a license under sub-section (1), by order, suspend such license (without waiting for completion of enquiry).	
	Duties of Certifying Authority	Sec 30 provides certain standards (called duties) to be maintained by Certifying Authority, which are:- Certifying Authority shall 1) Make secure use of hardware, software and procedure from intrusion and risk, 2) Provide a reasonable assurance about reliability of his services, 3) Adhere to security procedures (to ensure that secrecy and privacy of the ES are assured), 4) Be repository of all ESC, 5) Publish information regarding its practice, ESC and current status of such certificates and 6) Observe such other standards as may be specified by regulation (by the Controller) Failure to comply above standard may lead revocation or suspension of license by the controller u/s 25. Other duties:- 1) u/s 31, Certifying Authority is required to ensure that all person employed or engaged by him, observe and follow the provision of the act, the rules, the regulation and other order there under during the time of employment or engagement. 2) u/s 32(1), Certifying Authority is required to disclose - its Electronic Signature Certificate (which is also required u/s 30), - any certification Practice Statement (means a statement specify the practice that he employs in issuing ESC), - Notice of suspension or revocation, if any, and - Any other fact, which may be useful to evaluate the reliability of his product or service. 3) u/s 31(2), Certifying Authority is required, in the event or situation of where his integrity or security of computer system has been compromised, to inform such person which may be affected due to such event or take corrective action. 4) u/s 33, Certifying Authority is required to surrender the license to controller in case of suspension or revocation of license u/s 25. 5) Follow such other standards as may be specified by the Controller.	222 – 224
	Functions of Certifying Authority	Function of Certifying Authority are as below:- 1) u/s 35, Certifying Authority, subject to certain condition, grant DSC or reject the application after reasonable SCN. 2) u/s 36 Certifying Authority is required to certify that the Subscriber has to comply with the provision of the act, the rules, the regulations and other order there under. 3) u/s 37, the Certifying Authority has power to suspend DSC (for maximum 15 days), if he think it is necessary for public interest. The DSC can be suspended on application by subscriber or authorized person, 4) u/s 38, the Certifying Authority has power to revoke DSC, if in his opinion, the subscriber has submitted false statement or has canceled any material fact or the conditions subject to which DSC was issued was not satisfied. The DSC can be revoke in following cases also:- - application for revocation by subscriber or authorized person, - subscriber has become insolvent, - on death of subscriber, - subscriber being firm, has been dissolved, - subscriber being company, has been wound up - subscriber cease to exist by any reason. 5) u/s 39, the Certifying Authority is required to publish notice of suspension/revocation.	228 – 230
6.	Controller Means a person appointed u/s 17 by the Central Government.	Controller is appointed by the Central Government to supervise and direct the function of certifying authority. Section 17 provides that the Controller shall perform his function subject to general control and direction of the Central Government.	225
	Function of Controller (Sec 18)	Section 18 provides specific function, that controller may perform. Such are as below:- 1) Supervision of Certifying Authority 2) Certifying the Public Key of Certifying Authority 3) Laying down the standards to be followed by the Certifying Authority 4) Specifying the qualification and experience that a person has to posses to work in the officer of Certifying Authority, 5) Specify the conditions subject to which Certifying Authority can perform his functions, 6) Specify the form and content of ESC and the Key 7) Specify the form and manner in which accounts shall be maintained by the Certifying Authority, 8) Resolve the conflict between the Certifying Authority and their Subscribers 9) Laid down the duties of Certifying Authorities and 10) Maintain a database of all particulars of various Certifying Authority.	225 – 226
	Powers of Controller	The controller has various powers under the act. Some powers are as below:- 1) u/s 19, the controller has power (functional) to give recognition to Foreign Certifying Authority. 2) u/s 24, the controller has power (functional) to grant license to issue ESC or reject the application for license. 3) u/s 25, the controller has power to revoke or suspend license granted u/s 24 under certain cases (refer at **Para 221** for detail), 4) u/s 27, the controller has **power to delegate** his all power to any other officer of the office, 5) u/s 28, the controller **or authorized person** has all such powers that an Income Tax Officer has under chapter XIII of the Income Tax Act, 1961. 6) u/s 29, the controller **or authorized person** has power to access to computer or data of such person in the event of search, and direct them to assist them.	7
7.	Cyber Appellate Tribunal	CAT (previously, Cyber Regulation Appellate Tribunal) is established by the Central Government,	230 – 231

	Composition of CAT	CAT comprises one chairperson & such other number of members as may be prescribed by the CG	
	Qualifications of Chairperson	Person must be eligible to appoint as Judge of a High Court	
	Qualification of Judicial M.	Person must be member of the Indian Legal Service for a period not less than 1 year.	
	Qualification of Other Member	Special Knowledge of and experience (in information technology, telecommunication industry, management or consumer affairs) and Has hold govt. service at the post of :- - Additional Secretary or equivalent post for a period not less than 2 years or - Joint Secretary or equivalent post for a period not less than 7 years.	
8.	Electronic Signature and Electronic Signature Certificate	1) Means authentication of any electronic record by a subscriber by means of the electronic technique specified in the 2nd schedule of the act and includes Digital Signature. 2) DS means authentication of any record by a subscriber by means of an electronic method or procedure in accordance of Sec 3 (Sec 3 specifies the method or procedure for affixing the DS). 3) Electronic Signature Certificates means an ESC issued u/s 35 and includes DSC.	232
	Method and Procedure for affixing Digital Signature Section 3 provides the method and procedure for affixing digital signature.	Step 1 – E-record is created, a massage digest (say MD 1) is generated by applying "hash function" upon e-record. Hash Function digitally freezes the contents of record. The generated MD will be in alphanumeric form which will be unique for all files having same content. That means, if massage is altered, the revised MD will never be same as what was previously. Step 2- Massage Digest is encrypted by applying private key. Application of private key makes DSC affixed with MD. Such encrypted MD with record transmitted to appropriate receiver. At receiver place, the receiver perform following three task:- Task 1 – run hash function upon plain text record to generate MD (say MD 2), Task 2 – decrypt the encrypted MD to get MD 1. Task 3 – compare MD 1 with MD 2, if both are same, that means massage is not altered and securely reached to him.	232 – 234
	When any ES or Electronic Authentication technique shall be considered reliable..?	An electronic signature or electronic authentication technique shall be considered secure & reliable if:- 1) The signature creation data or the authentication data - Are linked to the signatory or the authenticator and not other person, - Were (at the time of signing or authenticating) under the control of the signatory or the authenticator, 2) Any alteration to the electronic signature (made after affixing such signature) is detectable, 3) Any alteration to the information made (after affixing the signature) is detectable 4) It fulfills such other condition which may be prescribed.	234 -235
	When a system considered secure..?	A secure system means, computer hardware, software and procedure that:- 1) Are reasonably secure from unauthorized access and misuse, 2) Provide a reasonable level of reliability and correct operation, 3) Are reasonable suited to performing the intended functions and 4) Adhere to generally accepted security procedures.	236
	When an E-record shall be deemed to be Secured..?	As per Sec 14, an e-record shall be deemed to be secured if the same are kept within such security procedures as may be prescribed. U/s 16, the CG is empowered to prescribe such security procedures.	247
	When an E-signature shall be deemed to be secured..?	As per Sec 15, an e-signature shall be deemed to be secured if, 1) At the time of affixing e-signature, the signature creation data was under controller of signature and not other person and 2) The signature creation data was stored and affixed in such manner as may be prescribed. U/s 10, the CG is empowered to prescribe the manner and procedure in which e-sign should be made.	
9.	Asymmetric Crypto System	Means a system of secure key paid consisting of a private key for creating DS and a public key for verifying the same.	235
10.	Key pair	Means, in an asymmetric crypto system, a private key and its mathematically related public key, which are so related that the public key can verify a DS created by the private key.	235
11.	Computer Contaminate	It refers to any set of intrusion that are designed to - Disrupt the operation of computer, computer system or computer network (by any means) or - Modify, destroy, record/copy or transmit "data or program stored in computer, computer system or computer network".	236
12.	Traffic Data	It refers to any data, identifying or purporting to identify any person, computer system, computer network, location (to or from communication is made or may be made and include origin), destination, route, time, data size, duration, type of service or any other information.	237
13.	Duties of Subscribers	Chapter VIII of the Act provides provision with respect to duties of subscriber:- 1) u/s 40, on acceptance of DSC, subscriber has to generate key pairs by applying security procedure 2) u/s 40A, it is provided that further duties may be prescribed, 3) u/s 41, it is provided that when will it deemed that DSC has been accepted and the consequences of such deemed acceptance. 4) u/s 42, it is provided that Subscriber should exercise all reasonable care to retain control of the Private Key and take care to prevent its disclosure. Where it private key has been compromised, he must communicate to Certifying Authority (till such communication, he will be liable for any offence or contravention through such DSC).	237
	Section 41	It shall be deemed that Subscriber has accepted DSC if he publish or authorize to publish such DSC in a repository or otherwise demonstrates his approval of the DSC. On acceptance of DSC, it will deemed that 1) the subscriber holds the private key (corresponding to Public Key published in DSC) and is entitled to hold the same 2) all representation made to the Certifying Authority are true, 3) all information in the DSC are within his knowledge and is true.	238
14.	Liabilities of Companies u/s 85	Section 85 provides that, in case of Offence by a Company, the person in charge shall be held liable and guilty for such offence or contravention unless he proves that the contravention or offence took place	239

		without his knowledge. Sub-section (2) of the section provides that, notwithstanding to sub section (1), where such offence or contravention taken place within knowledge of or due to neglect in the part of director, secretary or any other officer, such director, secretary or other officer shall be held guilty of offence and shall be punished accordingly.	
15.	Power of CG u/s 87	Refer study material Page 10.52	
16.	Cyber Regulation Advisory Committee	CRAC is a committee, established by the Central Government to advise - the CG wrt application of Act and - the Controller in framing the Regulation under the Act The Committee comprises 1 Chairperson and such Other Number of Members as CG deemed fit.	240
17.	Power of Police Officer to arrest persons.	1) Section 80 empowered the Police Officer and such other authorized officer (by CG or SG) to make search and arrest under the Act. 2) It provided that, any police officer not below the rank of Inspector can enter in any public place & search and arrest without any warrant. 3) It is further provided that such power can also be exercise by such officer as authorized by CS or SG but such officer is required to take such arrested person before the magistrate or officer in charge or a Police Station. 4) It is provided that Public Place means any place which is assessable to public and includes Hotel, Public Conveyance, shop etc.	241
18.	Compounding of Offence (It means payment of fine against punishment)	Section 77A provides the cases when a Court can compound an offence & which offence can't be. No offence shall be compounded 1) If the offence is repetitive (i.e. compounding is available once in life), 2) If the offence is against a child below 18 years or women, 3) If the punishment is for life or imprisonment for a term not less than 3 years, 4) If the offence affects socio-economic condition of the country.	242
19.	E-governance	Chapter III of the Act (sec 4 to 10) explain about the provisions wrt E-governance. 1) Sec 4 provides legal recognition to maintenance of records in electronic form subject to condition that such records must be accessible in future. 2) Sec 5 provides legal recognition to E-signature, if such signature is affixed in such a manner as may be prescribed (by CG u/s 10) 3) Sec 6 provides use of E-Signature and E-records by government and its agencies. Where any law requires filling of application, return or any other document or payment of any fee, tax or any other consideration to government or its agencies, the same shall be deemed so if made in electronic form (through internet) 4) Sec 7 provides that where any law requires maintenance of e-record for a certain period, the same shall be deemed to be satisfied if kept in e-form, remain assessable,, kept in required format and record of information about origin, destination etc also maintained. 5) Sec 8 provides legal validity to e-gazette. 6) Sec 9 provides that sec 6, 7 and 8 are not mandatory to comply. 7) Sec 10 provides power of CG to prescribe rules in respect of E-signature.	244 – 246
	Power of CG u/s 10 (wrt ES)	For the purpose of this Act, the Central Government may, by rules, prescribe:- 1) The type of Electronic Signature, 2) The manner and format in which ES shall be affixed, 3) The manner or procedure which facilitate identification of the person affixing the ES, 4) The control processes and procedures and 5) Any other matter, which is necessary to give legal effects to ES.	246
20.	Liability of Intermediaries Sec 2 defines intermediaries, in relation to any records, means • any person who - Receive, store or transmit records or - Provides any services wrt such records and • Includes - Telecom service provides - Internet service providers - Search engine - Online payment sites, - Online auction sites, - Online market place & - Cyber cafes	Sec 79 provides liabilities of Intermediaries wrt contents they publish or provide through any manner. An intermediary shall not be liable for any **third party information, data or communication link**, hosted by him if:- 1) The function of intermediary is limited to providing access to a communication system or 2) The intermediary does not • Initiate the transmission • Select the receiver of the transmission or • Select or modify the content of transmission. and 3) The intermediary observe due diligence while discharging his duties and also observe such other guidelines as the Central Government may prescribe. However, an Intermediary shall be held liable for its transmission of information or data if:- 1) It has conspired, abetted, aided or induced, whether by fraud or otherwise, in the commission of the unlawful act or 2) It, upon receiving actual acknowledgment or being notified by the appropriate government or its agency, that the contents hosted by him is being used to commit the unlawful act and the intermediary failed to remove such contents or failed to disable the access to that material.	248 – 250
21.	Attributes of E-records (Sec 11)	An e-record shall be attributed to the Originator if it was sent by - Himself or - A person duly authorized by him to send or - An information system programmed by him to send such e-record.	250 – 251
	Originator	A person who send, generate store or transmits any electronic massage/record or cause to send, generate, store or transmits to any other person, but does not includes an Intermediary.	

	Chapter – 8	**Information System Auditing Standards, Guidelines & Best Practice**	254 -
1.	ISO/IEC 27001-2005 (also called Information Security Management System)	- It is an Information **Security** Management System **Standard** given by the International Organization for Standardization (ISO) & The International Electro-technical Commission (IEC). - It **provides** various **specification (A) & standards (B)** for ISMS. - It also known as Part II of BS7799 Standard.	255 – 256
A.	Four Specifications of ISMS (also called Requirements of ISMS or Rules for protecting IS Assets)	1) General (general task provided to perform for IS security) 2) Management (task for management to perform for IS security) 3) Implementation (verification of task performed to ensure efficiency) and 4) Documentation (whatever performed, should be documented and recorded)	256 – 258
	1) General	The organization shall establish & maintain documented ISMS addressing 1) Assets (to be protected) and their classification on values basis, 2) Risk Management Approach, 3) Control objectives and controls and 4) Degree of assurance required.	
	2) Management (Establishing Management Framework, i.e. Rules for Management)	1) Define Information Security Policy 2) Define scope of ISMS 3) Make appropriate risk assessment, 4) Identify the areas of risk to be managed and degree of assurance required and 5) Select and implement appropriate controls	
	3) Implementation (verification)	This specification provides rules for 1) Verification of implemented controls and 2) Evaluation of efficiency and effectiveness of implementation procedure.	
	4) Documentation	This specification provides rules for documentation and maintenance of various task performed. The documentation shall consist of evidence of action undertaken for establishing following:- 1) Security Policy, 2) Control Implementation Procedure, 3) Verification procedure 4) Management framework summary, This specification further required that there should be proper controls over such documentations and their use.	
B.	Areas of focus of ISMS (ISMS aim to provide best practice to ensure security of the Information System.)	1) Security Policy 2) Organizational Security 3) Assets Classification and Controls, 4) Personnel Security, 5) Physical and Environmental Security 6) Communication and Operational Management, 7) Access Controls, 8) System Development and Maintenance, 9) Business Continuity Management and 10) Compliance	258
	1) Security Policy	This specifies that the organization should have a security policy for Information Assets. (**Refer 9.6**)	260
	2) Organizational Security	This standard specifies that the organization should establish a committee or group for implementation, maintenance and review of security controls implemented.	259
	3) Assets Classification	This standard requires the organization to 1) Maintain proper record of all information assets in a register with complete details called Information Assets Register and 2) Make classification of assets according to their value & importance to implement coherent controls.	
	4) Personnel (HR) Security	This standard requires the organization to maintain and implement proper rules for employees to minimize risk and threats associates with human errors. E.g. 1) Employment Agreement before joining, 2) Training for new comers, 3) Awareness Program, 4) Employees Ethics and Users access controls	
	5) Physical & Environment Security	This standard provides rules (called controls) for security of various organizational resources and information assets. This covers 1) Implementation of Controls to secure areas from unauthorized access, 2) Equipment Security and 3) General Controls	
	6) Communication and Operational Mgmt.	This standard provides rules for securing data stored & transmitted over network. This covers:- 1) Operational procedures and controls to ensure correct and secure operations 2) Protection against malicious codes and networking threats such as hacking, 3) Controls to maintain the integrity and availability of information. 4) Network management to safeguard data transmitted over network and ensure reliable & secure network.	
	7) Access Control	This standard specifies rules for access to information system resources and application. This covers:- 1) User access controls to prevent unauthorized access 2) Network access controls for protection of network from intrusion and hackers, 3) Application access controls to prevent unauthorized access to information held in IS, 4) Monitoring access to detect any unauthorized access	
	8) System Development and Management	This standard specifies rules for secure & effective development of system and its maintenance. This covers controls for system analysis (requirement analysis), system design and security of system files.	
	9) BCP Controls	This standard specifies controls to ensure continuity of business in the event of disaster or crises.	
	10) Compliance	This standard specifies rules for compliance with legislative system of the country, security policy drafted and other policies. This standard also specifies rules for regular review & audit of the system.	
2.	Capability Maturity Module	- The CMM is a methodology used to develop and refine processes of software development to achieve optimization therein. - The CMM aims to provide Optimum Software Process Capability. - The module describes five maturity levels.	
	11) Five levels of CMM	Level | Nature of Processes for Software Development | Process Outcome	

	The auditor who perform audit of SD processes to examine which level the organization belongs to, must have knowledge of such five levels in detail. If the organization is able to meet predetermined time and cost frame for development and develop a effective system, then organization may fall in Level 3 and if organization has capability to meet such outcome even in the event of happening of unwanted event, it will be classify as Level 4 Org. If organization has all feature to be categorized as level 4 org, and do further research and development for finding new approaches for SD, it will categorized as Level 5 Org.	1) Initial level	Disordered (chaotic), undocumented, ad hoc, uncontrolled, inconsistent, time consuming, inefficient.	Uncertain, beyond time and beyond cost.	
		2) Repeatable level	Documented but repeatable and inefficient.	Certain and within time but beyond cost.	
		3) Defined level	Well defined and documented set of standard processes but can't face any variance in resources.	Certain subject to availability of resources., within time and cost	
		4) Managed level	Quite mature and able to face uncertain fluctuation in availability of resources.	Certain even in case of variance in resources.	
		5) Optimized level	Enough optimized and force for new ideas for development	Well defined and certain in all cases.	
		Remarks:- 1) At level 1, the software processes are disordered, ad-hoc uncontrolled and time consuming. Because of such processes, the development of software also not certain and never achieve time and cost frame allocated for it. 2) At level 2, the processes are documented but repetitive. Developer meets the time frame but failed to meet cost frame as the processes repeated. 3) At level 3, the organization has well defined processes for software development but such processes does not have capability to meet uncertain event which are beyond controls and cause delay in software development beyond time and cost. 4) At level 4, the processes become quite mature enough to even meet the unexpected situation and brought desired outcome within predefined time and cost. 5) At level 5, the processes get complete maturity and become enough optimize and provides maximum benefit for development they can.			
	Software Process	A software process can be defined as set of actions and activities undertaken to develop and maintain software and associated products.			
	Software Process Capability	SPC describes the range of expected results that can be achieved by following software processes.			
	Software Process Maturity	SPM is the extent to which a specific process is explicitly defined, managed, measured, controlled and effective. Maturity implies a potential for growth in capability and indicates both the richness and consistency.			
3.	COBIT (Control Objectives for Information & related Technology)	- It is a **set of best practice for IT governance** developed by the Information System Audit and Control Association (ISACA) and IT Governance Institute, - It is a **good road map for IT governance**. - It is a globally accepted **set of tools** organized into a framework that and organization can use to ensure that their IT is helping them to achieve their goals and objectives. - It ensures the organization that Information Technology is working effectively to minimize IT-related risks and maximizes the benefits of technology investment. - It bridges the gap between the business and IT. - It includes an **Executive Summary** which provides a thorough awareness and understanding of its key concepts and principles. It also includes a synopsis of the **Framework** which provides a more detailed understating of its key concepts and principles while identifying COBIT's 4 domains and the 34 IT processes.				
	COBIT Framework	The COBIT Framework explains how IT processes deliver the information (information that the business needs to achieve its objectives). The framework identifies **seven criteria (of information)** as well as **IT resources** which are important for IT processes to support business needs. The COBIT Framework addresses the issue of control from three vantage points or dimensions:- 1) Business Objectives (To satisfy business objectives, information must conform to certain criteria that COBIT refer as business requirements for information. The criteria are divided into **7 distinct categories**.) 2) **IT Resources** (includes peoples, application system technology and infrastructure.) 3) IT Processes (which are broken into **4 domains**, Planning & Organizing, Acquisition & Implementation, Delivery & Support and Monitoring & Evaluation.)				
	7 Criteria of Information (that an Information must conform as per COBIT)	1) Effectiveness 2) Efficiency 3) Confidentiality	4) Integrity 5) Reliability	6) Availability and 7) Compliance	
	IT Resources	1) Peoples 2) Applications	3) Information and 4) Infrastructure		
	4 Domains/Area of COBIT	1) Plan and Organize (This domain provides rules for "planning for use of Information & Technology in to achieve the business goals and objectives.) 2) Acquire and Implement (This domains provides rules for acquisition and implementation of required Information Technology. This domain also provides development and maintenance plan to prolong the life of IT system and its components.) 3) Deliver and Support (This domain provides rules for delivery of efficient and effective services and support through the Information Technology.) 4) Monitor and Evaluate (This domain provides rules for regular monitoring and evaluation of Information Technology implemented.)			
	Benefits of COBIT	1) To Management, it provides rules to manage security of IT resources. It allows the management to benchmark the security and control practice, 2) To Users, it provides assurance that adequate security and controls exist and 3) To Auditors, it provides guidance to examine and comment upon security and controls exist and enable them to substantiate their opinion.			
	General benefits of COBIT	1) Provides a common language for executives, management and IT professionals			

		2) Enable working of business with IT for successful delivery of IT initiatives 3) Improved efficiency and optimization of cost 4) Reduced operational risk 5) More efficient and successful audits 6) Clear ownership and responsibilities, based on process orientation	
	Val-IT and COBIT	- Val IT is a complete framework covering value governance, portfolio management & investment management processes and activities. It helps enterprises make better decisions about where to invest, ensuring that the investment is consistent with the business strategy. - While COBIT ensures that IT is working as effectively as possible to maximize the benefits of technology investment.	
	Risk-IT and COBIT	- Risk IT is a complete framework covering risk governance, evaluation and response processes and activities. It provides a framework for enterprises to identify, govern & manage IT-related risks. Risk IT is used to enhance risk management. - While COBIT provides a set of controls to mitigate IT risk in IT processes.	
4.	*COSO* (Committee of Sponsoring Organizations of the Treadway Commission)	- *COSO* is an Internal Control Framework. - It defined internal control [as a process, (established by an entity's board of directors, management and other personnel) designed to provide "reasonable assurance" regarding the achievement of objectives] in the following category:- a) Effectiveness and Efficiency of Operations, b) Reliability of Financial Reporting and c) Compliance with applicable law and regulations	
	Five framework of *COSO* These components provide an effective framework for describing and analyzing the internal control system implemented in an organization.	5 essential component of *COSO* Internal Control Framework:- 1) Control Environment 2) Control Activities 3) Risk Assessment 4) Information and Communication and 5) Monitoring	
5.	*COCO* - Guidance on Control (Criteria of Controls)	- *COCO* is an Internal Control Framework (like *COSO*) for guidance on control. - This model is built on the concept of *COSO* framework by the Canadian Institution of CAs in 1995. - The *COCO* standard also called superset of *COSO* as it covers "the aspect of controls for information assurance in general" provided earlier by *COSO*. - *COCO* **describes internal control as actions** that foster (promote) the best result for an organization. These actions focus on a) Effectiveness and Efficiency of Operations, b) Reliability of Financial Reporting and c) Compliance with applicable law, regulations and internal policies	
	Four important concepts about Control provided by *COCO*	1) Control is affected by peoples (including the board of directors, management and other staff) in the organization, 2) Peoples who are accountable for achieving objectives of the organization should also be accountable for the effectiveness of controls, 3) Organization are constantly interacting and adapting, and 4) Controls can be expected to provide only reasonable assurance and not absolute assurance.	
6.	ITIL (IT Infrastructure Library)	- ITIL is an official publication of the Office of Government Commerce in the United Kingdom. - It is a set of practices for **IT Service Management** (i.e. ITIL is an ITSM Framework). - ITIL (the IT Infrastructure Library) is a series of documents that are used to aid the implementation of a lifecycle framework for IT Service Management. - The 2011 edition of ITIL consists of 5 core publications – Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service Improvement.	
	IT Service Management	- IT Service Management is a discipline of management for managing IT Systems. - It focuses upon providing a framework to structure IT-related activities and the interactions of IT technical personnel with business customers and users.	
	Five Volumes of ITIL V3	1) Service Strategy, 2) Service Design, 3) Service Transition, 4) Service Operation and 5) Continual Service Improvement	
	Eight Volumes of ITIL V2	ITSM sets relating to:- 1) Service Support 2) Service Delivery Other operational guidance relating to:- 3) ICT Infrastructure Management 4) Security Management, 5) The Business Perspective 6) Application Management 7) Software Asset Management To assist with the implementation of ITIL practice:- 8) Planning to Implement Service Management	
7.	SysTrust and WebTrust	- SysTrust and WebTrust are two specific services developed by the AICPA which are based upon the trust service principles and criteria. - SysTrust is an assurance service and certificate by CPAs which provides the assurance various stakeholders about the Information System of an organization that they are reliable and efficient. - WebTrust also is an assurance service and certificate by CPAs which concerned wrt reliability of network of the organization. - SysTrust applies to a wide variety of systems, while WebTrust focuses entirely on the Internet. - SysTrust examines the reliability of the systems themselves and WebTrust attests to controls over Internet-based transactions.	
	SysTrust Engagement	- In a SysTrust engagement, a CPA performs an examination (similar to an audit) to evaluate the system's reliability. - In a SysTrust engagement, a system is divided into following **four elements**:- 1) Infrastructure (such as hardware and facilities) 2) Software (including operating software, application software, utilities) 3) Procedure (which includes, IS backup procedure, maintenance procedure, input procedure etc.)	

		4) Data/Information (that system uses and support).	
	Five Principles relating to Trust Service Engagement (Five aspects to be considered by CPAs during audit under Trust Service Engagement) or (Five Focus area of SysTrust and WebTrust)	1) Security (Is system is protected from unauthorized access, logical as well as physical). 2) Availability (Does the system operates in accordance of business requirement? Is it assessable for routine processing and maintenance?) 3) Integrity (Does the system process information completely, accurately, in a timely manner, and in accord with the required authorization?) 4) Online Privacy (Does personal information obtained through e-commerce is collected, used, disclosed and retained as committed or agreed?) 5) Confidentiality (Does the information designated/classified as confidential protected?)	
	Reporting of Trust Service Engagement	After verifying above five aspect, a CPA express his opinion in following four areas:- 1) Policies (that the entity has defined and documented policies.) 2) Communications (that the entity has communicated its defined policies to authorized users.) 3) Procedures (that the entity uses the procedures, to achieve its objectives, in accordance with the defined policies.) 4) Monitoring (that the entity monitors the system and takes action to maintain compliance with its defined policies.)	
8.	HIPPA (The Health Insurance Portability and Accountability Act)	- HIPPA is an Act enacted by the US Congress in 1996, to administrate the health services in the country. It has two parts, Title I and Title II. - The standards are meant to improve efficiency and effectiveness of national health care system by encouraging widespread use of electronic data interchange in the US health care system.	
	Title I	Title I of HIPPA protects health insurance coverage for worker (of medical service providers) and their families when they change their jobs or lose their jobs.	
	Title II	- Title II of HIPPA requires the establishment of National Standards for Electronic Health Care Transactions and National Identifiers for providers, health insurance plan and employers. This part address the issues related to the security and privacy of health data. - **It requires the Department of Health and Human Services (HHS) to draft rules** to increase the efficiency of the health care system in the country. - It also defines numerous offenses relating to health care and sets civil and criminal penalties for them. It also creates several programs to control fraud and abuse within the health care system. - It also known as Administrative Simplification (AS) Provisions.	
	Rules under Title II of HIPPA As per the requirements of Title II, the HHS has promulgated 5 rules regarding Administrative Simplification:	1) The Privacy Rule (this Rule regulates the use and disclosure of Protected Health Information held by "covered entities") 2) The Transactions and Code Sets Rule (this rule provides standard for health care transactions and provision of Electronic Data Interchange), 3) The Security Rule [The Security Rule complements the Privacy Rule. However the Privacy Rule pertains to all Protected Health Information (PHI) including paper and electronic, the Security Rule deals specifically with Electronic Protected Health Information (EPHI)], 4) The Unique Identifiers Rule, and 5) The Enforcement Rule.	
	Types of Security Safeguards specifies by The Security Rule	1) Administrative Safeguard (provides policies and procedures to clearly show how the entity will comply with the Act.) 2) Physical Safeguard (requires controlling physical access to protect against inappropriate access to protected data.) and 3) Technical Safeguard (provides physical & logical controls to restrict access to IS.)	
9.	SAS 70	- SAS 70 is an internationally recognized Statement of Auditing Standards for Service Organization provided by AICPA. - SAS 70 provides guidance to independent auditors ("service auditor") to access the efficiency of internal controls of a Service Organization and issue an opinion through Service Auditor's Report. - SAS 70 is generally applicable when an auditor is auditing the financial statements of an entity (user organization) that obtains services from another organization (service organization). - SAS 70 allows the Service Organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format (Service Auditor's Report).	
	Service Auditor's Report	SAR is a report by Service Auditor expressing opinion on effectiveness and efficiency of internal control of a service organization. SAR also used by a Service Organization to disclose their control activities and processes to their customers and their customers' auditors in a uniform format.	
	Two types of Service Auditor's Report	1) Type I report describes the description of controls of Service Organization at a specific point of time. This form of report is used by SAR to provide details of control activities of Service Organization to their users and users' auditors. 2) Type II report, not only includes description of Service Organization's Controls, but also includes opinion on whether the specific controls were operating effectively during the period under review (i.e. opinion upon results of detailed testing of such controls over a minimum six months period).	
	Benefits of SAS 70 Report to the Service Organization	1) Service Organization receives significant value from having a SAS 70 report. 2) A SAR with an unqualified opinion by the auditor express that the Organization has effective control objectives and control objectives which differentiate it from its peers. 3) Without a current SAR, a service organization may have to entertain multiple audit requests from its customers and their respective auditors (this report serves as a single report for multiple purposes). 4) A SAR ensure users and users' auditors that all organization's users and user's auditor have access to control activities of service organization and that satisfy the requirement of Service Auditors.	
	Benefits of SAS 70 Report to the User Organization	User Organization that obtain a SAR from their Service Organization(s), receive valuable information about the control activities of the Service Organization.	

	Chapter 9	**Drafting of IS Security Policy & Audit Policy and IS Audit Reporting – A practical aspect**	
1.	IS Security	Information System security is essential to protect IS asset and resources. This involves security of physical and logical assets (refer **Para 139**).	266
	IS Security Objectives	For any organization, security objectives comprises following three attributes:- 1) Confidentiality (prevention of unauthorized disclosure of information) 2) Integrity (prevention of unauthorized modification of information) and 3) Availability (prevention of unauthorized withholding of information)	266 – 267
2.	Types of IS **Security Protection Program**	1) Preventive Protection (This type of protection requires safeguarding IS resources from any damage. It requires use of **Information System Security Controls**.) 2) Restorative Protection (this type of protection requires developing and maintaining backup and restore plans.)	270 – 272
	Types of IS Security **Preventive Protection** Controls	1) Physical Controls, such as Doors, locks, Entry Register, CCTV Guards etc., are intended to prevent unauthorized entry to IS location. 2) Logical Controls, such as Password, Firewall, Power Protection program etc., are intended to prevent unauthorized access to IS resources. 3) Administrative Controls, such as security policy, users' ethics etc., are those rules and regulation which are required to be followed by every internal parties to organization. It will be wrong to say that Physical Controls are intended to protection Physical Assets and Logical Controls are for protecting Logical Assets. On the contrary, Physical Controls also protect logical assets as they protect access to hardware containing such logical assets and Logical Controls prevent damage to hardware.	270 – 271
	Key question to be asked under **Restorative Protection** Program	1) Has the recovery process been tested recently? 2) How long the recovery process takes time? 3) How much productivity was lost? 4) Did everything go according to plan? 5) How much extra time needed to restore last changed back-up?	272
3.	Factors to be considered before opting an **IS Security Program**	1) All data do not have equal value. 2) Know where critical assets are reside (to implement an integrated security program) 3) Develop an access control methodology 4) Protect information stored in media and 5) Review hard output of employees' daily work.	269
4.	4 Rules to be followed before planning for Protection of IS	Rule 1 : We need to know "what the IS are" and "where these are located". This rule requires to know about IS and their locations. Rule 2 : We need to know "what is the value of IS" and "How difficult is to recreate or restore them". This rule requires to determine the value of IS and cost of restoration/recreation in case of damage or loss of them. Rule 3 : We need to know "who is authorized to access" and "what they permitted to do with IS". This rule requires to know who is authorized to access IS & up-to what extent modification is permitted and Rule 4 : We need to know "how quickly IS need made available when it becomes unavailable". This rule requires defining time frame for restoration.	269 – 270
5.	Factors critical to success of Business of an Organization	1) Strategic Plans (This includes various policies about the business of organization. The organization should keep their plans confidential. Most organization acknowledged that strategic plans are critical to success of their business but failed to provide reasonable controls to prevent their unauthorized disclosure. Unauthorized disclosure may cause significant loss to organization) 2) Business Operation (This includes such policies and procedures essential for daily operation of business. Some of such policies and procedures might be proprietary in nature. The organization should keep them safe from unauthorized access and disclosure.) 3) Financial Information (This includes all financial aspects about the business of organization. The organization should kept them secure to prevent competitive loss.)	267 – 268
6.	Security Policy	A policy is a plan or course of action designed to influence & determine decisions, actions and other matter. Similarly, an IS Security Policy is a set of action or activities to be undertaken for security of IS assets and resources.	273
	Types of IS Security Policy	1) Information Security policy (describes the definition of information security, its overall objectives and importance of security that applies to all users.) 2) Users Security policy (provides the responsibilities of users wrt security of IS.) 3) Acceptable Usage policy (set out acceptable email & internet service for the users.) 4) Organizational Information Security policy (set out group policy for security of its information assets and the IT system.) 5) Network and System Security policy (set out policy for system and network security and applies to IT department users.) 6) Information Classification policy (set of policy for classification of information assets.) 7) Condition of connection (set out the conditions to be comply by third party to connect with network of the organization.)	273
	Member of Security Policy (various group of management comprised by Security Policy)	Security Policy broadly comprises the following three group of management:- 1) Management Members (who have budget and policy authority), 2) Technical Members (who know what can and what cannot be supported) and 3) Legal Member (who know what is right or wrong in legal perspective)	279
	Issues to be address by security Policy	A model security policy should address following issues/aspects:- 1) Definition of Information System Security, 2) Definition of all relevant IS responsibilities (i.e. describe responsibilities of all users), 3) Reason why IS security is important, 4) Goals and principles of the policy and 5) Reference to supplementary documentation.	275
	Contents of IS Security policy	A typical IS Security Policy comprises following contents:-	274

	(the contents are somehow similar to Focus area of ISMS as provided **Para 256**, because both are about security of IS)	1) Purpose and Scope, 2) Security Organizational Structure 3) Responsibility Allocation 4) Assets Classification and Security Classification	5) Access Control 6) Incident Handling 7) Physical and Environmental Security 8) Business Continuity Management and 9) System Development and Maintenance Control.	
	Issues to be address under the herding "Responsibility Allocation"	1) Owner for each IS asset (i.e. who will held responsible for IS asset), 2) All staff should be aware of their responsibilities wrt security of IS assets, 3) All staff should be aware of importance of IS security, 4) All new network linked must be approved, 5) A list of contacts must be maintained, 6) Risk assessment of all third party access must be carried out.		275
	Asset Classification and Security Classification	1) An inventory (record) of IS assets and resources must be maintained, 2) A formal documented classification scheme must be in place and all staff must comply with it, 3) The owner (responsible person) should provide a security appropriate class, 4) The handling of information marked confidential or above mark, should be restricted, 5) Exchange of data between organization must be controlled, 6) Classified waste must be disposed of appropriately and securely		276
	Access Control	1) Access control must be in place, 2) The access controls must be audited at a regular basis, 3) Access must be granted in relation to business function only, 4) Access must be granted up-to the level required to perform normal business, 5) Each user must be provided unique identity for access, 6) A password policy should be defined, 7) Access rights must be deleted when user left or change the job,		276 – 277
	Incident handling	1) Security handling time and approach must be consistent at all time, 2) Procedure for collecting evidence relating to security incidents should be standard, 3) All staff must be aware of process, 4) Adequate record must be maintained.		277
	Physical and Environmental Security	1) Physical Security should be maintained 2) Security maintained should be checked regularly, 3) Access to important areas must be limited to authorized staff only, 4) Computer must never be left unattained showing important files, 5) Equipment, software or information must not be taken out off-site without proper authorization. 6) Confidential and sensitive information must be kept in lock if are not in use.		278
	Business Continuity Management	1) A BCP must be maintained, tested and updated, 2) All staff must be aware of BCP, 3) A business impact and business continuity assessment must be conducted annually.		278
	Role of IS Auditor wrt Security Policy	The IS auditor should ensure that 1) The IS policy is readily accessible to all employees, 2) The policy has an owner who is responsible for its maintenance and 3) The policy is updated		283
7.	IS Audit	Refer **Para 315**.		280
8.	IS Audit Policy	IS audit policy is a set of action and activities prepared to guide audit team to conduct an audit of Information System.		286
	Purpose of IS Audit Policy	IS audit policy is intended to guide audit team to successfully discharge their audit work.		286
9.	Audit Working Papers and Documentation	An audit working paper should record:- 1) The audit plan, 2) The nature of audit 3) Timing and extent of audit procedure 4) The conclusion drawn from the evidences obtain and 5) Other significant matters which requires exercise of judgment together with auditors' conclusion.		289
	Factors affecting contents of working papers	1) The nature of engagement, 2) The form of the auditor's report, 3) The nature of client business,	4) The complexity in client's business 5) The nature and condition of client's records and 6) Degree of assurance upon internal control system.	288
	Types of Working Paper	1) Permanent Audit Files (such files of set of files which are updated annually with information from current files. Such files contain information relating to all previous period of engagement.) 2) Current Files (such files which contains information relating to audit of current period only.)		288
	How to develop documented Audit Program	The documented audit plan is developed with the help of following activities:- 1) Documentation of audit procedures, 2) Objectives of the audit, 3) Scope nature and degree of testing required to achieve audit objectives, 4) Identification of technical aspects, risk processes and transactions which should be examined, 5) Procedures for audit will be prepared prior to commencement of audit work.		289

	Chapter – 4	**Testing – General and Automated Controls**	292 -
1.	Testing/Audit of Controls	Testing of controls involve obtaining the population and conducting the compliance tests of either entire population or selected sample from the population.	292
	Method of Testing	Testing may be of two types:- 1) Substantive Testing (this type of testing is used to substantiate the integrity of the actual processing. It is used to ensure that processes, not controls, are working as per the design of the control and produce the reliable results. 2) Compliance Testing (this type of testing is performed to determine whether controls are working effectively.)	292 – 293
	Phase in IS Control testing	1) Planning (The auditor determine an effective & efficient audit procedure to collect evidences.) 2) Testing (The auditor test the effectiveness and efficiency of IS Controls.) and 3) Reporting (The auditor then conclude his opinion on the basis of outcomes of testing phase.)	293
	Activities involved in IS Control Audit Process	1) Obtaining and understanding of entity and its operation/business, 2) Obtaining a general understanding of the structure of the entity's network, 3) Obtaining a preliminary understanding of IS Controls, 4) Identifying the key/critical areas of audit, 5) Assessing IS risk on preliminary basis, 6) Identifying critical control points, and 7) Performing other audit planning procedures.	294
2.	Factors assist IS Auditor to determine appropriate **Audit Procedure**	1) The availability of evidences outside the information system, 2) The relationship of information system controls to data reliability, 3) Accessing the effectiveness of IS Controls as an audit objective, and 4) The extent to which internal controls can be relied	294
	Contents of appropriate and effective **Audit Procedure** (Audit procedure for audit of IS Controls,, to analyze their effectiveness) (Appropriateness of Control Test)	To assess effectiveness of IS controls, the auditor should adopt a mix of audit procedure. Such audit procedure should include the following:- 1) Inquiries of IT and management staff, 2) Use of Questionnaire to obtain information on controls and how they are designed, 3) Observation of operation of controls, 4) Review of control documentation (such as control policies and procedures), 5) Inspection of approvals and authorization, 6) Data review of output of information system may provide evidences about the accuracy of processing, 7) Re-performance of controls, to test its effectiveness.	299
3.	Documentation of Preliminary Understanding of the design of IS Controls	The auditor should include following information in the documentation wrt preliminary understanding of design of IS Controls:- 1) Audit plan (that adequately describes the objectives, scope & methodology of the audit), 2) Identification of entity wide level and business process level controls designed to achieve the control activities and control activities for which no or ineffective controls are in place, 3) Determination of whether controls are designed effectively and implemented 4) Documentation for any significant computer related incidents identified and reported for the last year. 5) Status of the prior years' audit findings, 6) Relevant laws and regulations, 7) Security Policies and Plans, 8) Business Continuity Plans and Disaster Plans 9) Risk Assessment for relevant system. 10) Documentation of communication with entity management, 11) Audit resources planned, 12) Current **Multiyear Testing Plan**,	295 – 296
	Documentation of Control Testing Phase	The auditor should include following information in the documentation of Testing Phase:- 1) An understating of Information System that are relevant to the audit objectives, 2) IS controls objectives and activities relevant to the audit objectives 3) A description of control technique used at level (Entitywide, System and Business Process Application) and sublevel (Network, OS and IA), 4) Specific test performed for level and sub level controls, 5) Related documents describes the nature, timing and extent of testing 6) The conclusion about the effectiveness of controls and 7) For each weakness, whether material, significant or just a deficiency.	298 – 299
	Information to be documented by Auditor during identifying key area of audit	The auditor should identify "key areas" of audit, which are critical to achieving the control objectives. For each such area, the auditor should document relevant general support and major application files including:- 1) The operational location of each key systems or files, 2) Significant components of such key systems or files, 3) Other significant system or system level resources that support key systems or files, 4) Prior audit problems reported	300
4.	Test Effectiveness of IS Controls (Level of Controls)	The auditor should identify effectiveness of controls at each of the following levels:- 1) Entitywide or Component Level (General Controls, consist of processes designed to achieve the control activities. They are focused on how the entity or component manage IS related activities.) 2) System Level (General Controls, consist of processes for managing specific system resources related either a general support system or major application. These controls are more specific than those at the entity or component level and generally related to single type of technology.) 3) Business Process Application Level (Controls at business process application level consist of policies and procedures for controlling specific business processes.)	296 – 298
	Level under **System Level**	Within the system level there are three further levels:- 1) Network (a network is a interconnected or intersecting configuration or system of component.) 2) Operating System (an OS is software that controls the execution og computer programs and may provide various services.) 3) Infrastructure Application (IA are software that is used to assist in performing system operation,	297

		including management of network devices.)	
5.	Multiyear Testing Plan	Multiyear testing plan is a concept, the auditor adopt to 1) Reduce annual audit resources, 2) Allow the auditor to test computer related controls on a risk basis rather testing every control every year, 3) Perform some limited test and other activities annually, 4) Assure that all agency systems and locations are considered in the IS Control evaluation process, 5) Test different controls comprehensively every year. In a circumstances, where the auditor regularly performs IS Control audit, the auditor may determine that a multiyear audit plan for performing IS Control Audit is appropriate.	300 -301
	Limitation of MTP/MAP	Multiyear Audit Plan may not be appropriate in the following cases:- 1) First time audit 2) Audits where some significant business process application or general application are not been tested recently during last 3 years or 3) Audit of entities that do not have strong Entitywide controls,	301
6.	Concurrent on Continuous Audit Techniques	1) Continuous Audit techniques are such techniques used to collect evidences at the same time when an application system undertake a processing of it product data. 2) Continuous Audit techniques enable the auditor to significantly reduce the time between occurrence of processing of transaction and audit conclusion.	302
	Advantages of Continuous Audit Techniques	1) Timely, comprehensive and detailed auditing, 2) Provides features of surprise testing, 3) Provides information to system staff on meeting of objectives of controls, 4) Training for new users.	302 – 303
	Limitation/disadvantages	1) Costly to implement and maintain, 2) Auditor needs to have knowledge of working within the computer systems, 3) Auditor should be able to obtain sufficient resources required to support the technique 4) The techniques are more likely to be used where audit trail is not visible, 5) The techniques are more likely to be used if auditor is involved in the development work and 6) The techniques are likely to be effective if they are implemented in an application system.	303
	Basis for collective evidences	The continuous audit techniques uses two basis for collecting audit evidences:- 1) Special Audit Module embedded in the application system or system software, to collect, process & print audit evidences (Snapshoot techniques and Integrated Test Facility), 2) Special Audit Records, stored in application system files or a separate audit file. Such records are used to store the audit evidences collected, so that the auditor can examine them at later stage (SCARF and Continuous & Intermittent Simulation)	304
	Various Continuous Audit Techniques	1) Snapshoot Technique, 2) Integrated Test Facility, 3) SCARF and 4) Continuous and Intermittent (i.e. irregular) Simulation	
7.	Snapshoot Technique	1) It is a concurrent audit technique used by IS auditor to evaluate authencity, accuracy and completeness of transaction processed by an Information System. 2) This technique involves use of software paced in the application software to capture picture of transaction processing. 3) The auditor then access the authencity, accuracy and completeness of the processing by scrutinizing the snapshoot (picture) taken by the software. 4) This techniques requires the auditor to make following three decisions:- 1) Where to place the snapshoot software in the application system. 2) When the software will capture snapshoot of transaction and 3) Timing and format of reporting by the software.	304 – 305
8.	Integrated Test Facility	1) The ITF is a concurrent audit technique used by IS auditor to evaluate authencity, accuracy and completeness of transaction processed by an Information System. 2) This technique involves introduction of dummy entity within the application system and processing test data against the dummy entity to verify processing authencity, accuracy and completeness. 3) Dummy entity means, where the application system is a payroll system, a fictitious person or where the application system is a inventory system, a fictitious stock. 4) The presence of ITF transaction affects the actual output of the application system and thus the effect of such transaction has to be removed. 5) Using ITF involves following three decisions to be taken by auditor:- 1) What method will be used to enter the test data? 2) What method will be used to remove the effect of ITF Transaction?	306 - 307
	Method to enter Test Data into Application System	1) The first method involves tagging transaction. The application system must be programmed to recognize the tagged transaction or 2) The second method involves designing new test transaction and entering them with the production data into the application system.	
	Approach/method to remove or minimize effect of ITF transaction.	1) Modify the application system to recognize ITF transaction and ignore them,, 2) Submit additional input that reverse the impact of the ITF transaction or 3) Submit trivial (small) entries to minimize the effect of such transactions.	
9.	SCARF	1) SCARF stands for System Control Audit Review File. 2) It is the most complex concurrent audit technique used by IS auditor to evaluate authencity, accuracy and completeness of transaction processed by an Information System. 3) This technique involves embedding audit software module within a host application system to provide continuous monitoring of system transaction and keeping record in a special audit file called SCARF. 4) Where the module find any exceptional transaction,, it immediately report it to auditor and provide direct evidence through printing the details. 5) In many ways, the SCARF is like Snapshoot Technique. 6) Using SCARF involves two major questions:- 1) What information will be collected by software module embed and	308

		2) What reporting system is to be used with SCARF.	
	Information to be collected by SCARF:-	1) Application System Errors (where any system error occurred, SCARF will collect information about it and will store it into special file) , 2) Policy and procedural variance, (where it is found that any transaction is not as per security policy or other policy and procedure, the same will be stored in SCARF), 3) System Exception (certain exception are allowed, however where exceptions increased beyond accepted level, the same shall be reported through SCARF) 4) Statistical Sample, 5) Snapshoot and extended records, 6) Profiling Data and 7) Performance Measurement data	308
	Determining the structure of SCARF reporting	The following decisions are involved in determining the structure of reporting under SCARF:- 1) How SCARF files will be updated? 2) Choosing short codes and report formats to be used and 3) Choosing the timing of report preparation	309
10.	Continuous and Intermittent Simulation (CIS)	1) The CIS is a concurrent audit technique used by IS auditor. 2) It is considered as a variant of SCARF. 3) This technique can be used to trap exception whenever the application system uses a DBMS.	309 - 310
	Execution of CIS During application system processing, CIS executed in the following way:-	1) The DBMS read the application system transaction. 2) DBMS passed it (transaction) to CIS, 3) CIS then determine whether further examination is necessary, if yes, the nest step are performed otherwise, it continued to receive further transaction. 4) CIS replicates or simulate the application system processing 5) Every update to database is checked by CIS and 6) Exceptions identified by the CIS are written in a log file called Exception Log File.	309 – 310
	Advantage of CIS	It does not require modification to the application system and yet provides an real-time auditing capability.	
11.	Reviewing the Network (LAN)	The review of controls over Network is done to ensure that ▪ Standard are in place for designing and selecting a LAN architecture and ▪ Cost of establishing network does not exceed benefits there from.	311
	Items to be review Understanding these information enable the auditor/ reviewer to make an assessment of the significant threats to the LAN.	1) LAN topology and network design,, 2) Significant LAN components (such as modem and server) 3) LAN uses, 4) LAN Administrator,, 5) Significant groups of LAN users, In addition to above, the reviewer should gain the understanding of following:- 1) Functions performed by LAN administrator, 2) The company's division or department procedure and standards relating to the network, and 3) LAN transmission media and techniques.	311

	Chapter – 3	**Control Objectives**	
1.	IS Auditing	IS auditing is a process of collecting and evaluating evidences, to determine whether an IS ▪ Safeguard the IS assets and resources, ▪ Maintain Data Integrity, ▪ Allows organization to achieve goals effectively and ▪ Use of resources efficiently.	315
	Purpose of IS Audit (Audit Objectives)	An IS Audit may be conducted 1) To ensure integrity, confidentiality and availability of information system and resources, 2) To ensure protection of the entire system from common security threats and 3) To ensure the following other objectives:- ▪ Safeguard the IS Assets and resources, ▪ Maintenance of data integrity ▪ Maintenance of system effectiveness ▪ Ensure system efficiency and ▪ Compliance with IS related policies, guidelines, circulars etc.	282
	Scope of IS Audit	The scope of IS auditing should encompass the examination and evaluation of - The adequacy and effectiveness of the system of internal controls and - The quality of performance by the information system.	280
	Need for IS Auditing	Information system audit is necessary because of following objectives:- 1) Assets Safeguarding (The IS Assets, like other assets, should be protected from various threats.) 2) Data Integrity (It means maintenance of certain attributes of data such as completeness, accuracy, purity and veracity. If data integrity is not maintained, organization has no longer true picture about itself.) 3) System Effectiveness (It means to ensure that IS provides information for which it was developed.) 4) System Efficiency (It means to ensure that IS uses resources efficiently in optimized manner.)	315 – 317
	Role (Responsibility) of IS Auditor	1) The IS Auditor shall be responsible for establishing control objectives that reduce or eliminate potential exposure to control risk, 2) The auditor should review the audit subject and evaluate the review results to find out are for improvement and 3) The auditor should submit a report to the management with his recommendation for improvement.	282
	Functions of IS Auditor	The IS Auditor reviews **risk relating to the IT system** and process. The IS auditor performs all such functions necessary to achieve audit objective .	283
	Risk related to IS System	1) Inadequate Information Security, 2) Inefficient use of corporate resources or poor governance, 3) Ineffective IT strategies, policies & practice and 4) IT related frauds	283
	Type of IS/IT Audit IT Audit has been categorized into five types:-	1) System and Application Audit (an audit to verify that system and application are appropriate, efficient and effective & proper controls are in place.) 2) Information Processing Facilities Audit (an audit to verify that all processing facilities are well controlled to ensure accurate and efficient processing.) 3) System Development Audit (an audit to verify that developed system has achieved its objectives and system was developed according to generally accepted development standards.) 4) Management of IT and Enterprise Architecture Audit (an audit to verify that IR Management has developed an Organizational Structure and Procedure to ensure controlled & efficient processing environment.) 5) Telecommunication, Intranet and Extranet Audit (an audit to verify that controls are in place on the client, service of the organization and on the network connecting the client and server.)	287
	Steps in IS Audit IS audit procedure can be grouped into six stages:-	1) Scoping and Pre-audit Survey (under this stage, the auditor determined the main area of focus and such areas which are not material to review.) 2) Planning and Preparation (under this stage, on the basis of outcome of 1st stage, the auditor prepare a plan for audit work to be execute.) 3) Fieldwork (under this stage, the auditor collects evidences by application of various techniques.) 4) Analysis (under this stage, the auditor analysis collected evidences using various analytical tools.) 5) Reporting (under this stage, the auditor draft his opinion in standard format called report and submit it to management.) 6) Closure (at this last stage, the auditor maintained documentation of collected evidences and conclusions.)	288 – 289
	Contents of Audit Report	1) Cover and Title Page, 2) Table of Contents 3) Summary/Executive Summary, 4) Introduction, 5) Findings, 6) Opinion and Appendices	286
2.	Effect of Computer upon Audit	Duce to change in organizational system from manual to computerized, the audit procedure also gets changed to face changed environment. Audit involves two basic task, collection of evidences and evaluation of such evidences. Change in system leads change in approach of collection of evidence and evaluation techniques.	
	Change to Audit Evidences	In a manual system, the auditor has visible audit trail to collect required audit evidences. However, in a computerized system, audit trail does not available everywhere. Where they are not, the auditor needs to opt other approach for collection of evidences. To collect audit evidences in a computerized environment, the auditor has two approaches for collecting audit evidences, Auditing around the computer and Auditing through the computer.	323
	Change to Audit Evaluation	It is a second task performed by auditor to trace any deficiency or weakness with the information system. In case of manual audit, the auditor evaluates evidences using various analytical techniques. However, to evaluate a information system process, such techniques are not much useful. This leads auditors to use Computerized Auditing Tools.	324
3.	IS Controls	A control is a system that prevents, detect and correct unlawful events. There are three aspects in the	324

		definition of controls:- ▪ Control is a system, ▪ It focus upon unlawful events and ▪ It is used to prevent, detect or correct unlawful events.	
	Need for Controls	1) Cost of Organizational Data (Data are critical resources necessary for continuing operations. Controls are implemented to protect such data from destruction.) 2) Value of Hardware, Software and Personnel (In addition to data, computer hardware, software and personnel are also critical resources and their loss may have significant effect upon viability of the organization. Controls are implemented to protect them from unauthorized access.) 3) Incorrect Decision Making (The quality of decisions based upon the information supplied by the information system. Controls are implemented to ensure effective and efficient working of IS to improve quality of decision making.) 4) Cost of Computer Abuse (Unauthorized access to IS resources may cause destruction of IS assets and resources. To prevent unauthorized access, proper controls are required.) 5) High cost of Computer errors (Absence of appropriate control may lead errors in computer system, the cost/loss of which may be very high.) 6) Maintenance of Privacy (Lack of appropriate controls may lead compromise with data integrity of the system. To maintain privacy, there must be proper controls.)	314
4.	Effect of Computer on Internal Controls Change in organizational system from manual to computerized lead major effect upon Internal Controlling System. However, the **basic principles** remained same; the way of controlling gets changed from manual to computerize. Basic Principles of Internal Controlling System:- ▪ Segregation of duties, ▪ Delegation of authority and responsibility ▪ Documentation and record keeping, ▪ Physical access control ▪ Recruitment and training of high quality staff & ▪ Management supervision	1) Segregation of Duties (In a manual system, single person was entrusted single task to prevent any error and provide compensatory control. However, in a computerized environment, it will be ineffective to provide one program for one task only. Since, a single program is capable of performing many task, the segregation of duties wrt task does not required. However, this component of Controlling required segregation of duties wrt IT Staff. The authorization to work with computer system should not be provided to person authorized for computer programming and vice-versa.) 2) Delegation of Authority and Responsibility (In a computerized environment, it is a difficult task to trace who is responsible for a particular task as many systems are used on sharing basis. However, still there should be proper delegation of authority and responsibilities wrt various ARE to prevent unauthorized access and make owner accountable for any unusual activity.) 3) Recruitment and Training of High Quality Personnel (In a manual system of controlling, it is general practice to employ trustworthy employees to maintain data integrity. The same principle applied wrt computerized environment.) 4) Adequate Documentation and Record (Like a manual system, in a computerized system of controlling, proper documentation and records should be maintain. However, the way of maintenance gets changed from manual to electronic.) 5) Physical Access Control (In a manual system, to restrict physical access, general physical controls were in use. The changes into computerized system lead use of electronic technology such as biometric system to restrict physical assess up-to authorized persons.) 6) Management Supervision (In a computerized system of controlling, the way of monitoring subordinated also changed into electronic mode. In a manual system, the supervision task was performed by physical appearance. The introduction of electronic equipments, such as video conferencing, CCTV etc. enables the management to supervise subordinates.)	317 – 322
	Component of Internal Controlling System	Internal Controls comprises five interrelated components:- 1) Control Environment (Elements that establish the control context in which specific accounting system and control procedures must operate.) 2) Risk Assessment (Elements that identify and analyze the risk faced by an organization and the ways these risks can be managed.) 3) Control Activities (Elements that operate to ensure transactions are authorized, duties are segregated adequate documentation and record maintenance, assets safeguard etc principles of Internal Controls.) 4) Information and Communication (Elements in which information is identified, captured and exchanged in a timely manner.) and 5) Monitoring (Elements that ensure working of internal controls reliably over time.)	322
5.	Control Implementation Cost	Implementation and Operating Controls involves following five cost:- 1) Initial Cost (This cost is incurred to design, develop and implement controls.) 2) Executing Cost (This cost is associated with working of controls.) 3) Correcting Cost (This cost is associated with correcting errors and malfunctions identified by control activities.) 4) Failure Cost (This cost is loss occurred from errors and malfunctions not identified by control activities.) and 5) Maintenance Cost (This cost is associated with ensuring reliable working of controls over time.)	325
6.	Types of IS Controls	Various IS Controls can be classified on the basis of their Objectives, Nature or Functional level.	
	Based on Objectives	1) Preventive Controls - These are controls intended to prevent materialization of any threat and occurrence of any loss to IS. Characteristics of Preventive Controls ▪ A clear understanding of vulnerable areas of IS, ▪ Understanding of probable threats and ▪ Provision of necessary controls for probable threats. 2) Detective Controls – These are controls intended to detect any unlawful activities within the information system and report. Characteristics of Detective Controls ▪ Clear understanding of lawful activities to identify any deviation to be report as unlawful. ▪ An established mechanism for reporting of identified unlawful events to proper person, ▪ Interaction with preventive controls to avoid reoccurrence and ▪ Surprise checks by supervisor	325 – 327

		3) Corrective Controls – These are controls designed, developed and implemented to remove or minimize the impact of threats which has materialized. ▪ Minimize the impact of threats, ▪ Identify the cause of threats, ▪ Correct errors arising from a problem, ▪ Modify the system to avoid reoccurrence of threats and problems. 4) Compensatory Controls – Where the organization is not able to implement appropriate controls due to some constraints (like lack of appropriate staff to maintain, financial problem etc.), the organization must ensure that there should be some compensatory control which at least will minimize the impact of threats.		
	Types of Controls on the basis of Nature of IS resources they are applied	1) Environmental Controls 2) Physical Access Controls, 3) Logical Access Controls, 4) IS Operational Controls	5) IS Management Controls 6) System Development & Acquisition Controls 7) System Implementation Controls 8) User Controls	328
	Based on Functions (as identified by auditors in review of Control System)	1) Internal Accounting Controls – Controls which are intended to safeguard the client's assets and ensure reliability of financial records. 2) Operational Controls – Controls which deals with day to day operation, function and activities to ensure such operation, activities and functions are contributing to business objectives. 3) Administrative Controls – Controls which are concerned with compliance of policies & procedures.		328
7.	Data Coding Errors – Types	1) Addition (Addition of extra character in a code. e.g. 54329 is coded as 543291) 2) Truncation (Omission of a character in a code. e.g. 54329 is coded as 5432) 3) Transcription (Coding wrong character. e.g. 54329 is coded as 54319) 4) Transposition (The position of characters changed. e.g. 54329 is coded as 54239) 5) Double transposition (The position of more than one character changed. e.g. 54329 is coded as 52439)		329
	Factoring affecting Coding Errors	1) Length of Codes, 2) Characters of Codes (B sound like V) 3) Alpha-numeric Mix Code 4) Mixing of UPPER case and lower case 5) Sequence of character.		330
8.	Service Level Agreement	SLA is a formal agreement between a customer requiring services and the organization that is responsible for providing those services. A SLA should define/provides following:- 1) The level of user demand to be satisfied, 2) Standard f service to be provided, 3) The level of technical support to be provided, 4) The procedure for providing service, 5) Emergency requirement 6) A schedule of charges		
	Contents as per auditors' view	An auditor should ensure that SLA should have following contents:- 1) Service provider should comply with all legal requirements 2) SLA should provide a "right to audit" clause, 3) The extent of responsibility of the service provider, 4) Insurance requirement		332
9.	User Final Acceptance Testing	It ensures that the functional aspects as expected by the users have been incorporated in the developed system. The testing aims to provide users the confirmation that:- 1) The user requirement specification has been met, 2) End user and operational documentation is accurate, comprehensive and usable, 3) Back-up and recovery procedures work effectively		
	Testing involve in UFAT	▪ Performance Testing ▪ Stress or Volume Testing ▪ Security Testing, ▪ Clerical Procedures Checking, ▪ Back-up and Recovery Testing		332 – 333
10.	Information Classification	The classification of information is important to provide appropriate level of controls and other measures according to their sensitivity and value.		333
	Various class of Information	▪ Top Secret Information ▪ Highly Confidential Information ▪ Proprietary Information,	▪ Internal Use Only and ▪ Public information	333 – 334
11.	Category of Data Integrity Controls	1) Source Data Control, 2) Input Validation Controls, 3) Online Data entry controls,	4) Data processing and storage controls, 5) Output controls and 6) Data transmission controls	334
	Data Integrity Policies	▪ Virus Signature Updating, ▪ Software testing, ▪ Division of environment	▪ Offsite backup storage and ▪ Disaster Recovery	334
12.	Data Security	Data security encompasses the protection of data from accidental or intentional disclosure to unauthorized person or unauthorized modification and deletion.		335
	IS Auditor's responsibility	An IS auditor should evaluate the following to access the adequacy of controls over data integrity:- 1) Who is responsible for the accuracy of data? 2) Who is authorized to access the data? 3) Who is authorized to change or modify the data? 4) Who is permitted to update the data? 5) Who control the security of data? 6) What contractual penalties or remedies are in place to protect tangible and intangible exposure?		335

13.	Crypto System	It refers to a suit of algorithm needed to implement a particular form of encryption and decryption.				336
	Asymmetric Crypto System	It refers to set of key pair consisting of private key for encryption and public key for decryption.				
	Algorithm in Crypto System	1) Algorithm for key generation, 2) Algorithm for encryption and 3) Algorithm for decryption				336
	Cipher	Cipher refers to set of algorithm for encryption and decryption - a series of well-defined steps that can be followed as a procedure.				336
14.	Data Encryption Standard	DES is a standard prescribing encryption algorithm. It is a method for encrypting information selected as an official Federal Information Processing Standard (FIPS) in the US in 1976 and later it become international wide standard. It is a mathematical algorithm for encrypting and decrypting binary coded information. Encrypting algorithm encrypts the data into unintelligible form called **Cipher** and decrypting algorithm decrypt the data into plain text. An authorized user of encrypted data must have the key that was used to encrypt data, in order to decrypt the data.				336 – 337
15.	Public Key Infrastructure	When utilizing PKI policies and controls the financial institution need to consider the following:- 1) Defining the method of initial verification appropriate for different types of certificate applicants. 2) Define the controls for issuing digital signature and key pairs, 3) Select an appropriate certificate validity period, 4) Ensure that digital signature certificates are valid, 5) Define the circumstances for authorizing a certificate's revocation, 6) Updating database of revoked certificates 7) Employing stringent measures to protect the root key 8) Requiring regular independent audit 9) Regularly reviewing exceptional reports and 10) Ensuring that institution's certificates & authentication system complies with widely accepted PKI standards.				337 – 338
16.	Firewall	▪ A firewall is a set of components that mediate between internal domain and external domain. ▪ All traffic between domains passes from firewall, inward or outward, irrespective of the flow, ▪ Typically firewalls blocks or allows traffic based on rule configured by the administrator. ▪ Firewalls are subject to failure, however, upon failure, they block all traffic rather allowing all traffic to pass.				338 – 339
	Types of Firewall	1) Packet Filtering Firewall, 2) Stateful Inspection, 3) Proxy Server Firewall and 4) Application Level Firewall				339
	Packet Filtering Firewall	Network layer firewalls, also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set. The firewall administrator may define the rules; or default rules may apply. Network layer firewalls generally fall into two sub-categories, stateful and stateless. Stateful firewalls maintain context about active sessions, and use that "state information" to speed packet processing.				
	Stateful Inspection					
	Proxy Server Firewall	A proxy server (running either on dedicated hardware or as software on a general-purpose machine) may act as a firewall by responding to input packets.				
	Application Level Firewall	Application-layer firewalls work on the application level of the TCP/IP stack. Application firewalls function by determining whether a process should accept any given connection. Application firewalls work much like a packet filter but application filters apply filtering rules (allow/block) on a per process basis instead of filtering connections on a per port basis.				
	Characteristics	PFF	SIF	PSF	ALF	
	- Inspection	Packet header only	State of connection	Intermediary only	Packet head and contents also	
	- Usage	Small office or home OS	Network Inbound Traffic	Domain name server, web server	Telnet, FTP, HTTP	
	- Scope	Enforce security one	Based on the request from the firewall	A layer of access control	Additional screening of packets	
	- Advantages	Faster performance than ALF	Like PFF	Cache required and response to provide performance benefit	Strong level of security	
	- Limitation	Low security	Stateful filtering pre-defined rules	Employed behind other firewall	Time consuming	
17.	Hacking	Hacking is an act of penetrating computer system to gain knowledge about the system, system contents and system working. There are four ways in which hacking can be performed:- 1) NetBIOS, 2) FTP, 3) HTTP, 4) RPC Statd and 5) ICMP Ping (Internet Control Message Protocol Ping)				343
	NetBIOS Hacking	This is worst kind of hacking as it does not requires having any hidden backdoor program in the system. NetBIOS is meant to be used LAN, so machines on that network can share information. Unfortunately, the bug is that NetBIOS can also use across the internet.				
	FTP Hacking	FTP stands for file Transfer Protocol. It is used to download files from websites. If we have own website, FTP may be used to upload files from own computer to internet. FTP can also be used by hacker.				

	HTTP Hacking	HTTP stands for Hyper Text Transfer Protocol. This hacking can be harmful only if we use MS Web Server Software as this software has a bug called "unchecked buffer overflow" cause hacking.	
18.	Virus	A virus is a program (usually destructive) that attaches itself to a legitimate program to penetrate the operating system in a number of ways. One common technique that virus uses to penetrate is simply replicate itself over and over within the memory and destroy data. Virus program usually attaches with the following types of files ▪ .exe or .com program files, ▪ .ovl (overlay) program files, ▪ The boot sector of a disk or ▪ A device driver program.	
19.	Worms	Worms are malicious program which does not requires a host like a Trojan Horse requires. A worm copies itself to reduce memory space in the disk. Since worm are stand alone program, they are easy to detect. Worms can also be used to perform some useful task, e.g. worms can be used to establish a network.	345 – 346
20.	Trojan Horse	Trojan Horses are malicious programs hidden under any host program. A Trojan horse may ▪ Change or steal the password or ▪ Modify records in protected files, or ▪ Allow illicit (illegal) users to use the system. Trojan Horse cannot copy itself to other software like worm and virus can. Trojan gets activated only when host program activated. Trojan horse hides in a host program and generally does not damage the host program.	346
21.	Bombs	Bomb is a piece of code planted by an insider or supplier of a programmer intentionally. The bombs explode when the condition of explosion get fulfilled. However these programs cannot infect other program until exploded. Types of Bomb:- 1) Time Bomb – It is like a physical time bomb in logical form. It gets exploded when the pre-fixed time triggered. The computer clock initiates it. 2) Logical Bomb – It is a bomb which activated by combination of event.	347
22.	Personal Identification numbers (PIN)	A secret number will be assigned to the individual, in conjunction with some means of identifying the individual, serves to verify the authenticity of the individual. The visitor will be asked to log on by inserting a card in some device and then enter their PIN via a PIN keypad for authentication. His entry will be matched with the PIN number available in the security database.	
23.	Auditor's role in Logical Access Control	An IS auditor should keep the following points in mind while working with logical access control mechanisms:- 1) Reviewing the relevant documents pertaining go logical facilities and risk assessment and evaluation techniques and understanding the security risks facing the information processing system. 2) The potential access paths into the system must be evaluated by the auditor and documented to assess their sufficiency. 3) Deficiencies or redundancies must be identified and evaluated. 4) By supplying appropriate audit techniques, he must be in a position to verify test controls over access paths to determine its effective functioning. 5) He has to evaluate the access control mechanism, analyze the test results and other auditing evidences and verify whether the control objectives have been achieved. 6) The auditor should compare security policies and practices of other organizations with the policies of their organization and assess its adequacy.	
24.	Auditor's role in Physical Access Control	Auditing physical access requires the auditor to review the physical access risk and controls to form an opinion on the effectiveness of the physical access controls. This involves the following: 1) Risk assessment: The auditor must satisfy himself that the risk assessment procedure adequately covers periodic and timely assessment of all assets, physical access threats, vulnerabilities of safeguards and exposures there from. 2) Controls assessment: The auditor based on the risk profile evaluates whether the physical access controls are in place and adequate to protect the IS assets against the risks. 3) Planning for review of physical access controls. It requires examination of relevant documentation such as the security policy and procedures, premises plans, building plans, inventory list and cabling diagrams. 4) Testing of controls: The auditor should review physical access controls to satisfy for their effectiveness.	