Notes on MICS

July 13

2009

These notes are for students preparing for Paper 6 (Old Course) of CA final examination conducted by the Institute of Chartered Accountants of India. **To know how best a student can prepare for this subject, how to use these notes, tips to score maximum marks, etc. pls. read FAQ.pdf in the Files section at** **http://groups.yahoo.com/group/micsca** For queries/suggestions feel free to reach the author at nsshah@sjshah.in

[Past Exam Questions up to Nov - 2008 covered]

I N D E X

Chapter I: *BASIC CONCEPTS OF SYSTEMS*

1. System :
The term system may be defined as a set of interrelated elements that operate collectively to accomplish some common purpose or goal.

2. Boundary :
The features that define and delineate a system form its boundary. The system is inside the boundary; the environment is outside the boundary.

3. Subsystem :
A subsystem is a part of a larger system. Each system is composed of subsystems, which in turn are made up of other subsystems, each sub-system being delineated by its boundaries.

4. Interfaces :
The interconnections and interactions between the subsystems are termed interfaces.
The number of interconnections if all sub systems interact is in general $\frac{n(n-1)}{2}$
Each interconnection is a potential interface for communication among subsystems.

5. Cohesion :
The extent to which a system unit-subroutine, program, module, component, subsystem-performs a single dedicated function. Generally**, the more cohesive are units, the easier it is to maintain and enhance a system**, since it is easier to determine where and how to apply a change.

6. Coupling :
Measure of interconnectivity among software program modules' structure. Coupling depends on the interface complexity between modules. This can be defined as the point at which entry or reference is made to a module, and what data passes across the interface. In application software design, **it is preferable to strive for the lowest possible coupling between modules**. Simple connectivity among modules results in software that is easier to understand, maintain and less prone to a ripple of domino effect, caused when errors occur at one location and propagate through a system.

7. Decomposition / Factoring :
The process of decomposition of subsystems into smaller subsystems until the smallest subsystems are of manageable size -is called Factoring.

8. Systems Entropy :
Systems can run down and decay or can become disordered or disorganized. Stated in system terminology, an increase in entropy takes place.
Preventing or off setting the increase in entropy requires inputs of matter and energy to repair, replenish, and maintain the system. This maintenance input is termed as negative entropy.

9. **Supra System** :
It refers to an entity formed by a system and other equivalent systems with which it interacts (i.e. the system above it).

10. System Stress :
A stress is a force transmitted by a system's supra-system that causes a system to change, so that the supra-system can better achieve its goals. In trying to accommodate the stress, the system may impose stress on its subsystems, and so on.

Types of Stress:
1. Change in goal set of system
2. Change in achievement levels desired.

Consequences of Stress:
To accommodate stress or it will become pathological i.e. it will decay and terminate.

11. Information :
Information is data that have been put into a meaningful and useful context.

12. Redundancy :
It means the excess of information carried per unit of data. For example, 75% of the letters used in a phrase are usually redundant.

13. Transaction Processing Systems :
Transaction Processing Systems are aimed at expediting and improving the routine business activities that all organisations engage.

14. Management information system (MIS) :
An organized assembly of resources and procedures required to collect, process and distribute data for use in decision making.

15. Decision support systems (DSS) :
An interactive system that provides the user with easy access to decision models and data, to support unique (non-recurring) & semi structured decision-making tasks.

16. Executive information systems (EIS) :
They enable executives to extract summary data from the database and model complex problems without the need to learn complex query languages, enter formulae, use complex statistics, or have high computing skills.

17. Expert systems :
Expert systems have arisen largely from academic research into artificial intelligence. An expert system has a built in hierarchy of rules which are acquired from human experts in the appropriate field. Once input is provided the system should be able to define the nature of the problem and provide recommendations to solve the problem. The expert system should be able to learn, i.e. change or add new rules. They are developed using very different programming languages such as PROLOG which are referred to as fifth generation languages.

18. Types of Systems :

i. Deterministic i.e., it operates in a predictable manner, e.g. Computer program; and Probabilistic system i.e., can only be described in terms of probable behaviour with a degree of error always attached to the prediction of what the system will do, e.g. an inventory system.
ii. Closed, relatively closed and open systems.

19. Characteristics of Information:

1. Timeliness: It is a mere truism to say that information, to be of any use, has to be timely.

2. Purpose: The basic purpose of information is to inform, evaluate, persuade, and organise.

3. Mode and format: Format of information should be so designed that it assists in decision making, solving problems, initiating planning, controlling and searching.

4. Redundancy: It means the excess of information carried per unit of data. For example, 75% of the letters used in a phrase are usually redundant.

5. Rate: The rate of transmission/reception of information may be represented by the time required to understand a particular situation.

6. Frequency: Represents number of times the information transmitted.

7. Completeness: The information should be as complete as possible.

8. Reliability: Information should have indication of confidence level.

9. Cost benefit analysis: The benefits that are derived from the information must justify the cost incurred in procuring information.

10. Validity: It measures the closeness of the information to the purpose which it purports to serve.

11. Quality: Quality refers to the correctness of information.

Year of Exam	Question No.	Chapter No.	Ans. Page No.	Marks	Question
May-03	[2(b)]	1	1.7-1.8	10	Explain the concept of decomposition with the help of an example.
May-04	[7(d)]	1	1.17	5	Write short note : Expert systems
Nov-05	[2(b)]	1	1.10	5	Define the term system stress and system change.
May-06	[2(a)]	1	1.10-1.14	10	What do you mean by Information? Describe the important characteristics of information which makes it useful to the organization.
May-07	[6(c)]	1	1.5-1.6	5	Differentiate between open and closed system.
Nov-07	[2(b)]	1	1.15-1.17	10	System analysts develop various categories of information systems to meet a variety of business needs. Discuss any three such systems briefly.
May-08	[7(a)]	1	1.5-1.6	5	Write short note: Closed and open systems.
Nov-08	[7(d)]	1	1.17	5	Write short note : Expert systems.

Chapter II: *TRANSACTION PROCESSING SYSTEM*

1. Transaction File :
A transaction file is a collection of transaction input data. Transaction files usually contain data that are of temporary rather that permanent interest.

2. Master File :
A master file contains data that are of a more permanent or continuing interest.

3. Reference or Table file :
A reference or table file contains data that are necessary to support data processing. Common examples of reference files used in data processing are payroll tax tables and master price lists.

4. Batch processing :
The processing of a group of transactions at the same time. Transactions are collected and processed against the master files at a specified time.

5. Real-time processing :
An interactive online system capability that immediately updates computer files when transactions are initiated through a terminal.

6. Transaction Processing Cycle :
A transaction processing cycle organises transactions by an organisation's business processes. The nature and types of transaction processing cycles vary, depending on the information needs of a specific organisation. Nevertheless, most business organisations have in common, transactions that may be grouped according to four common cycles of business activity.

a. Revenue cycle: Events related to the distribution of goods and services to other entities and the collection of related payments.

b. Expenditure cycle: Events related to the acquisition of goods and services from other entities and the settlement of related obligations.

c. Production cycle: Events related to the transformation of resources into goods and services.

d. Finance cycle: Events related to the acquisition and management of capital funds, including cash.

Financial reporting cycle: - NOT an operating cycle. It obtains accounting and operating data from other cycles and processes these data in such a manner that financial reports may be prepared. Valuation and adjusting entries are required to be made, e.g. Depreciation and currency transactions.

7. Components of the transaction processing system :

a. Inputs: Source documents, such as customer orders, sales slips, invoices, purchase orders, and employee time cards. Source documents are typically forms carefully designed for ease of use and accurate data capture.

b. Processing: Processing involves the use of journals and registers to provide a permanent and chronological record of inputs. Journals are used to provide a chronological record of financial transactions.

Sales journal: used to summarize sales made on account.
Purchase journal: used to summarize purchase made on account.
Cash receipts journal: used to summarize receipts of cash.
Cash disbursements journal: used to summarize disbursements of cash.
The design of special-purpose journals is one of the most important steps in the design of an accounting system.
Computer Processing:
Batch Processing: The processing of a group of transactions at the same time. Transactions are collected and processed against the master files at a specified time. The flow of processing in a batch processing computer system is essentially same as in a traditional manual system-source documents to journals (transaction files), journal to ledgers, and ledgers to financial statements.
Direct Processing: An interactive online system capability that immediately updates computer files when transactions are initiated through a terminal. In direct processing, individual transactions are posted directly to ledgers rather than being batched to build a transaction file.

c. Storage: Data is stored in what is called as a file. A file is an organized collection of data.
Master file: A collection of records pertaining to one of the main subjects of an information system, such as customers, employees, products and vendors. Master files contain descriptive data, such as name and address, as well as summary information, such as amount due and year-to-date sales.
Following are the kinds of fields that make up a typical master record in a business information system. There can be many more fields depending on the organization. The "key" fields below are the ones that are generally indexed for matching against the transaction records as well as fast retrieval for queries. The account number is usually the primary key, but name may also be primary. See transaction file for examples of typical transaction records.

```
     EMPLOYEE MASTER RECORD
key  Employee account number
key  Name (last)
     Name (first)
     Address, city, state, zip
     Hire date
     Birth date
     Title
     Job class
     Pay rate
     Year-to-date gross pay

     CUSTOMER MASTER RECORD
key  Customer account number
key  Name
     Bill-to address, city, state, zip
     Ship-to address, city, state, zip
     Credit limit
     Date of first order
     Sales-to-date
     Balance due
```

Transaction file: A collection of transaction records. The data in transaction files is used to update the master files, which contain the data about the subjects of the organization (customers, employees, vendors, etc.). Transaction files also serve as audit trails and history for the organization. Where before they were transferred to offline storage after some period of time, they are increasingly being kept online for routine analyses.

Following are the kinds of fields that make up a typical transaction record in a business information system. There can be many more fields depending on the organization. The "key" fields below are the ones that are generally indexed for fast matching against the master record. The account number is usually the primary key, but name may also be used as a primary key. See master file for examples of typical master records.

```
     EMPLOYEE PAYROLL RECORD
key  Employee account number
     Today's date
     Hours worked

     ORDER RECORD
key  Customer account number
     Today's date
     Quantity
     Product number

     PAYMENT RECORD
key  Customer number
     Today's date
     Invoice number
     Amount paid
     Check number
```

d. Output: Any document generated in the system is an output. When planning a new system, the developers usually start by designing the outputs from the system. Outputs, then, drive the inputs to AIS. E.g. of Outputs Trial Balance, Financial Reports etc.

Year of Exam	Question No.	Chapter No.	Ans. Page No.	Marks	Question
May-07	[5(c)]	2	2.1	5	What is Transaction processing cycle? Discuss briefly four common cycles of a business activity.

Chapter III: *BASIC CONCEPTS OF MIS*

1. Management information system (MIS)

An organized assembly of resources and procedures required to collect, process and distribute data for use in decision making. (Source: CISA Review Manual 2003)

It is a network of information that supports management decision-making. The role of MIS is to recognize information as a resource and then using that resource for effective and better achievement of organisational objectives.

2. Characteristics

a) Management oriented : It should start from an appraisal of management needs and overall business objectives.

b) Management directed : It is necessary that management should actively direct the system's development efforts. The implemented system meets the specifications of the designed system. In brief, management should be responsible for setting system specifications.

c) Integrated: All the functional and operational information sub-system should be tied together into one entity.

d) Common data flows: Data is captured by system analysts only once and as close to its original source as possible.

e) Heavy planning element: An MIS usually takes 3 to 5 years and sometimes even longer period to get established firmly within a company.

f) Sub system concept: It must be broken down into digestible sub-system which can be implemented one at a time by developing a phasing plan.

g) Common database: It is defined as a "superfile" which consolidates and integrates data records formerly stored in many separate data files.

h) Computerised: use of computers increases the effectiveness of the system.

3. Misconceptions / Myths about MIS :

1. Study of MIS is about the use of computers.
2. More data in report means more information to management.
3. Accuracy in reporting is of vital importance.

4. Pre-requisites of an effective MIS

a) Database: A stored collection of related data needed by organisations and individuals to meet their information processing and retrieval requirements. It can be defined as a "superfile" which consolidates data records formerly stored in many data files. The data in database in organised in such a way that accesses to the data is improved and redundancy is reduced.

i) User-oriented
ii) Common data source
iii) It is available to authorised persons only.
iv) It is controlled by a separate authority established for the purpose, known as Data Base Management System (DBMS)

b) Qualified system and management staff :
   i) Systems and Computer experts and
   ii) Management / Functional experts

c) Support of Top Management : It should receive the full support of top management.

d) Control and maintenance of MIS: Control of the MIS means the operation of the system as it was designed to operate. Some time, users develop their own procedures or short cut methods to use the system, which reduce its effectiveness. To check such habits of users, the management at each level in the organisation should devise checks for the information system control.
Maintenance - There are times when the need for improvements to the system will be discovered. Formal methods for changing and documenting changes must be provided.

e) Evaluation of MIS :
   i) Flexibility exists in the system, to cope with any expected or unexpected information requirement in future.
   ii) Ascertaining the views of users and the designers about the capabilities and deficiencies of the system.
   iii) Guiding the appropriate authority about the steps to be taken to maintain effectiveness of MIS.

5. Constraints in operating MIS :

1. Non-availability of experts, who can diagnose the objectives of the organisation and provide a desired direction for installing and operating system.
2. Experts usually face the problem of selecting the sub-system of MIS to be installed and operated upon.
3. Non-standardised approach in designing and implementing MIS.
4. Non-availability of cooperation from staff is a crucial problem.
5. High turnover of experts in MIS.
6. Difficulty in quantifying the benefits of MIS, so that it can be easily comparable with cost.

6. Effects of using Computer for MIS:

1. Speed of processing and retrieval of data increases :
   Unbelievably fast computational capability and systematic storage of information with random access facility has emerged as an answer to the problems faced in modern day's management. Moreover, retrieval of information in relevant form and design when needed in considerably less time and facilitates the management action and decision making.
2. Scope of use of information system has expanded :
   Multiple type of information for varied purposes can now be provided by using an on line real time system to various users sitting at a remote distance from a centrally located computer system.
3. Scope of analysis widened :

Such information equips an executive to carry out a thorough analysis of the problems and to arrive at the final decision.

4. Complexity of system design and operation increased
The need for highly processed and sophisticated information based on multitudes of variables has made the designing of the system quite complex.

5. Integrates the working of different information sub-system :
A suitable structure of management information system may be a federation of information sub-system, viz., production, material, marketing, finance, engineering and personnel. This common data base may meet out the information requirements of different information sub-system by utilising the services of computers for storing, processing, analysing and providing such information as and when required.

6. Increases the effectiveness of Information system :
Information received in time is of immense value and importance to a concern and this makes the concern more effective.

7. Limitations of MIS:

1. Output of MIS basically governed by quantity of input and processes.
2. Not a substitute for effective management.
3. May not have requisite flexibility.
4. Cannot provide tailor made info packages suitable for type of decision made by executives.
5. Takes into account mainly quantitative factors.
6. Less useful for making non-programmed decisions.
7. Effectiveness of MIS reduced in organisation where the culture of hoarding into and not sharing with others.
8. Effectiveness decreases due to frequent as in top management operational structure and operational team.

8. Establishing information needs in Management Process:

In general the planning information requirements of executives can be categorised into 3 broad categories: -

1. Environment information:
   i. Government policies
   ii. Factors of production
   iii. Technological environment
   iv. Economic trends
2. Competitive Information :
   i. Industry demand
   ii. Firm demand
   iii. Competitive data
3. Internal Information :
   i. Sales forecast
   ii. Financial plan/budget
   iii. Supply factors
   iv. Policies vital for subsidiary planning at all levels of organisation

9. Factors on which information requirements depend :

1. Operational function : The grouping or clustering of several functional units on the basis of related activities into a sub-system is termed as operational function. The content

of information, in fact, depends upon the activities performed under an operational function.

2. Type of decision making :

a) Programmed decisions: Are decisions on issues by reference to a predetermined set of precedents, procedures, techniques and rules. Not much judgment and discretion is needed in finding solutions to such problems.

b) Non-programmed decisions: Are those, which are made on situations and problems which are novel and non-repetitive and about which not much knowledge and information are available. They are non-programmed in the sense that they are made not by reference to any pre-determined guidelines, standard operating procedures, precedents and rules but by application of managerial intelligence, experience, judgment and vision to tackling problems and situations, which arise infrequently and about which not much is known. Government policy changing drastically, competitor's new entry, etc.

3. Level of management activity:

a) Strategic Level: Strategic level management is concerned with developing of organisational mission, objectives and strategies. Decisions made at this level of organisation to handle problems critical to the survival and success of the organisation.
Information Required: To make long term plans, policy matters and broad objectives of the company, the strategic level of management requires information on:
i) Trends
ii) Forecasts of the future
iii) Summary and 'exception reports'

Information requirement at top level for making decision

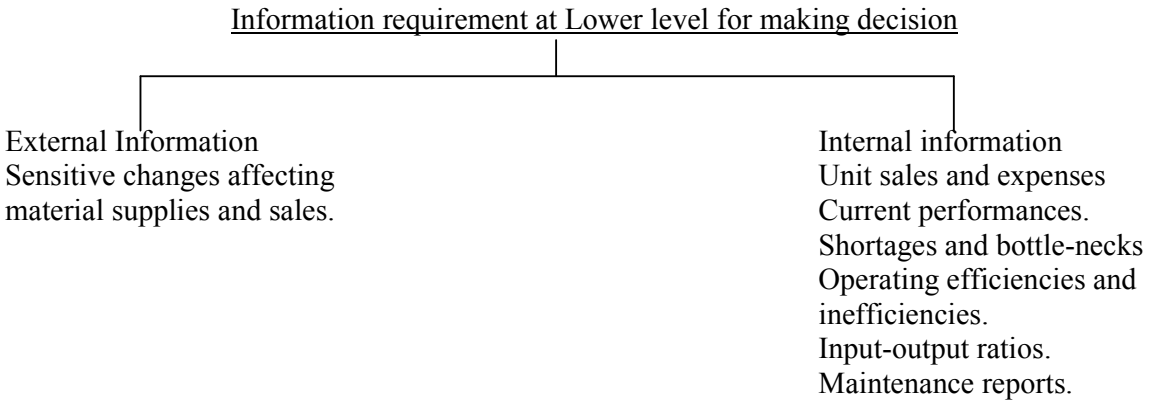
External	Internal
Competitive Activities	Historical-sales, costs
Customer preferences, style, changes	Profit, cash flow, divisional, income, sales, expenses.
Economic trends	Financial ratios, interests; credit outstanding,long-termdebt,delinquent accounts.
Technological changes, legal rulings	Projects' progress reports and cost updates.

b) Tactical Level: Tactical level lies in middle of managerial hierarchy. It consist of heads of functional departments and chiefs of technical staff and service units. Manager of sales, the manager of purchasing, finance manager, and the manager of personnel etc. At this level, managers plan, organise, lead and control the activities of other managers.
Information Required: A Middle management position is fed with information both from top management and supervisory management.

Information requirement at middle level for making decision

External	Internal
Price changes; shortages	Descriptive information (happenings)
Demand or supply, credit conditions.	Current performance indicators.
	Over-under budgets.
	Historical profits, sales, income.

c) Supervisory Level: This is the lowest level in managerial hierarchy. The managers at this level coordinate the work of others who are not themselves managers. They ensure that specific tasks are carried out effectively and efficiently. It consist of section officers, office managers and superintendents, foreman and supervisors who are directly responsible for instructing and supervising the efforts of clerical and 'blue collar' employees and workers.
Information required: They are required to make routine, day-to-day decisions that do not require much judgement and discretion. They mostly need internal information on operational aspects of the functioning of activity units. The nature of information is routine and structured.



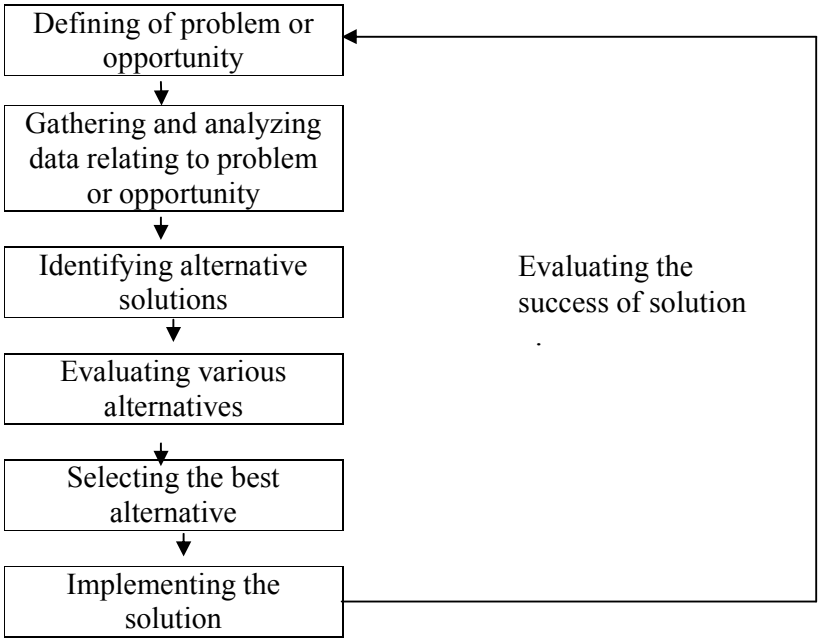
Year of Exam	Question No.	Chapter No.	Ans. Page No.	Marks	Question
Nov-02	[2(a)]	3	3.16-3.18	8	Differentiate among Strategic, Tactical and Operational categories of Information required for different levels of Managerial decision-making.
May-03	[2(a)]	3	3.9-3.11	10	Discuss the effect of applying computer technology to Management Information System.
Nov-03	[2(b)(ii)]	3	3.16,3.17,3.18	6	Mention at least two pieces of information-one internal and one external-required at every one of the levels of Management.
Nov-03	[2(b)(i)]	3	3.14-3.15	3	Describe briefly three levels of Management
May-04	[2(c)]	3	3.12 – 3.13	10	Explain three board categories of the planning information requirements of executives.
Nov-04	[7(a)]	3	3.14 - 3.15	5	Write short note : Strategic and Tactical decisions
May-05	[2(c)]	3	3.6-3.8	5	Describe the main pre-requisites of a Management Information System which makes it an effective tool.
May-06	[1(c)]	3	3.11	5	Discuss the limitations of the management Information System.
Nov-06	[2(a)]	3	3.4-3.6	10	State the factors to be considered for designing the effective Management Information System.
May-08	[2(b)]	3	3.6-3.8	10	Describe the main prerequisites of a MIS which makes it an effective tool. Explain the major constraints in operating it.
May-08	[7(b)]	3	3.13-3.14	5	Write short note: Programmed decisions.
Nov-08	[5(c)]	3	3.8	10	XYZ company engaged in manufacturing and installing power plant equipments has installed a new MIS and you have been requested to evaluate its effectiveness. On what parameters would you evaluate the MIS system?

Chapter IV: *SYSTEMS APPROACH AND DECISION MAKING*

1. Systems Approach to management :

It visualises an organisation as a group interacting and interdependent parts with a purpose. **Before solving problem in any functional area, or in any specific sector of the organisation, he should understand fully how the overall system would respond to changes in its component parts.**

a) Defining of the problem
b) Gathering and analysing data concerning the problem
c) Identification of alternative solutions
d) Evaluation of alternative solution
e) Selection of the best alternative
f) Implementation of the solution



2. Classification of decisions:

1) Programmed and Non-Programmed decision
2) Strategic and Tactical decision
3) Individual and group decision:

a) Individual decision: Individuals assume full responsibility for the consequences of such decisions. They may get information, factual analytical reports, from their subordinates or from specially established committees. But the responsibility and authority or the onus of making the final decision rests with the concerned manager himself. He cannot delegate or abdicate the authority of decision making.

b) Group decisions: are those, which are made by, more than one manager joining together for the purpose. Get enrichment by the pooling of diverse expertise, knowledge, authority and perspectives represented by the group up.

3. Decision Making through MIS : Some ex:

1. Computer model can be used to stimulate an industry segment and find company's potential for a share of market and profitability

2. Financial model to test impact of ideas and strategies on future profitability and to determine the needs for funds and physical resource
3. To carry out risk analysis & sensitivity analysis.

4. Decisions made in various functional areas with the help of MIS:

1. Finance and Accounting
   a) Estimation of requirement of funds
   b) Capital Structure Decision – To select optimum mix of different sources of capital
   c) Capital Budgeting – Decisions on investment in different assets
   d) Profit Planning – Financial decisions concerning profits and dividends, to ensure adequate surplus in future for growth and distribution of dividends
   e) Tax Management – Reducing outflow of cash resources by way of taxes.
   f) Working Capital Management – Investment of long term funds into current assets
   g) Current Assets management – Policy decisions regarding various items of current assets. E.g. credit policy

5. Various functional areas and sub-systems:

1. Production
   a) Production Planning – determining what should be produced, when it should it be produced and how it should it be produced.
   b) Production Control – includes the control of all activities related to expediting, coordinating and controlling the operations of various production departments
   c) Production scheduling – Planning the specific time at which product items should be manufactured.
   d) Materials requirement planning – MRP's purpose is to greatly improve both inventory management and production scheduling. It integrates several production related system so that it can access and extract data from these systems.

2. Marketing
   a) Sales Management – Would include Sales support and Sales Analysis
   b) Market Research and Intelligence – to investigate problems confronting the other managers in marketing function
   c) Advertising and Promotion – Planning and executing advertising campaigns to accomplish overall sales objective of marketing management.
   d) Product development and planning – analyzing possible opportunity for a new product and evaluating preferred specification and probable market success.
   e) Product Pricing
   f) Customer Service – provides customers with technical assistance and product maintenance.

3. Personnel
   a) Recruitment – Forecast personnel needs and skills required. Also maintains inventory of skills available.
   b) Placement – Matching available persons with requirement.
   c) Training and Development – Constantly updating workforce in new techniques and development.
   d) Compensation – determine pay and other benefits
   e) Maintenance – designed to ensure that personnel policies and procedures are achieved
   f) Health and safety – Health of personnel and safety of jobs

Year of Exam	Question No.	Chapter No.	Ans. Page No.	Marks	Question
May-03	[3(b)]	4	4.8-4.9	10	Discuss various benefits which are attained by implementing a computerized model for making decision.
Nov-03	[2(a)]	4	4.13-4.14	8	Explain the role played by Financial Information System in making financial decisions.
May-03	[7(d)]	4	4.24	5	Write short note : Materials Requirement Planning (MRP)
Nov-03	[2(b)(iii)]	4	4.9-4.10	3	Discuss the potential impact of computers and MIS at the top level of Management.
May-04	[5(b)]	4	4.25-4.27	6	Discuss various sub-systems of PIS, which are responsible to increase its operational efficiency.
May-04	[5(a)]	4	4.24-4.27	2	"The Personnel information system is the backbone of any organisation" Explain
Nov-04	[2(a)]	4	4.21-4.23	10	What are the production information requirements of a GM (Production and Operations Management) with regard to production planning and control?
Nov-04	[2(b)]	4	4.27	5	What are the variables that the top management should consider during negotiations with the labour unions?
May-05	[4(a)]	4	4.14-4.19	10	A Company is planning to introduce a new range of products. The top management is advised to get developed on marketing information system which can enhance the decisional capacities in various marketing activities. You being in-charge of this project suggest what information sub-systems are required to be developed.
Nov-05	[2(a)]	4	4.1-4.3	10	How systems approach can be used for solving problems?
May-06	[2(b)]	4	4.19-4.20	5	"Information is necessary to executive for performing the function of planning" Substantiate the above statement with regard to information requirements of marketing system.
May-06	[2(c)]	4	4.13-4.14	5	Describe various decisions which can be made with the help of financial information system.
May-06	[7](iii)	4	4.24	5	Write Shot notes on any four of the following: (iii) Material requirements planning
Nov-06	[2(b)]	4	4.15-4.16	10	Enumerate various information which are required for sales support and sales analysis.
Nov-07	[1(c)]	4	4.8-4.9	5	Discuss any five benefits which are attained by implementing a computerised model for making decisions.

May-08	[5(c)]	4	4.24-4.25	5	"Personnel information system deals with flow of information relating to people." Explain.
Nov-08	[3(a)]	4	4.11-4.14	10	What is Financial decision making? Which Financial decisions are made with the help of Financial information system?

Chapter V: *DECISION SUPPORT AND EXECUTIVE INFORMATION SYSTEMS*

1. What is a DSS?

A DSS can be defined as an interactive system that provides the user with easy access to decision models and data, to support semistructured decision-making tasks. It provides tools to managers to assist them in solving semistructured and unstructured problems in their own, somewhat personalized, way. DSS supports the human decision making process, rather than providing a means to replace it.

2. Characteristic of DSS

1. They support semistructured or unstructured decision-making
2. They are flexible enough to respond to the changing needs of decision makers, and
3. They are easy to use.

a) Semistructured and Unstructured Decisions :
The problem is first defined and formulated.
It is then modeled with DSS software.
Next, the model is run on the computer to provide results.
The modeler, in reviewing these results, might decide to completely reformulate the problem, refine the model, or use the model to obtain other results.
Example, simulating cash flows under variety of business conditions by using financial modeling software. Depending on results, the user might decide to completely remodel the problem, run the model under a number of new assumptions or accept the results

b) Ability to adapt to changing needs :
Do not conform to a predefined set of decision-making rules. Enough flexibility to enable users to model their own information needs. Relatively unsystematic and distinctive. Variety of tools. Formulas, functions, sorts, graphs, formal models, and so on.

c) Ease of Learning and Use :
Operated by users rather than by computer professionals, the tools that accompany them should be relatively easy to learn and use. Such software tools employ user-oriented interfaces such as grids, graphics, non-procedural fourth-generation languages (4GL), natural English and easily read documentation.

3. Components of a DSS:

1) The users :
Usually a manager with an unstructured or semi-structured problem to solve. No extensive education in computer programming. The planning language is nonprocedural, meaning that the user can concentrate on what should be accomplished rather than on how the computer should perform each step.

2) Database :
   a) One or more
   b) Internal and / or external

3) Planning languages :
   a) General purpose:

General purpose planning languages allow users to perform many routine tasks-for example, retrieving various data from a database or performing statistical analyses.

b) Special-purpose:
Special-purpose are more limited in what they can do

4. Model base :
The model base is the "brain" of the decision performs data manipulations and computations with the data provided to it by the user and the database. The model base, or model base management system (MBMS), contains one or more models for the kind of analysis the system will perform. For example, if the purpose of the system is to supply sales projections under different conditions, one model might be a linear regression formula derived from past sales and other factors.

4. Executive Information system (EIS):

EIS is a tool that provides direct on-line access to relevant information in a useful and actionable information about aspects of a business that are of particular interest to the senior manager.
They are specifically tailored to executive's information needs.
They are able to access data about specific issues and problems as well as aggregate reports.
They provide extensive on-line analysis tools including trend analysis, exception reporting.
They can access a broad range of internal and external data.
They are particularly easy to use (typically mouse or touch-screen driven)
Information tends to be presented by pictorial or graphical means.
Information is presented in summary format with facility to "drill down" to detail level
EIS require large amounts of capacity and processing power within both the system and the network.

5. Characteristics of Types of Information used in Executive Decision making:

1. Lack of structure
2. High Degree of Uncertainty.
3. Future oriented
4. Informal sources.
5. Low level of detail

6. Purpose of EIS:

(i) The primary purpose of an Executive Information System is to support managerial learning about an organization, its work processes, and its interaction with the external environment. Informed managers can ask better questions and make better decisions.
(ii) A secondary purpose for an EIS is to allow timely access to information.
(iii) EIS could give managers and subordinates an opportunity to work together to determine the root causes of issues highlighted by the EIS. The powerful focus of an EIS is due to the saying "what gets measured gets done." Managers are particularly attentive to concrete information about their performance when it is available to their superiors. This focus is very valuable to an organization if the information reported is actually important and represents a balanced view of the organization's objectives.

Year of Exam	Question No.	Chapter No.	Ans. Page No.	Marks	Question
Nov-02	[2(b)]	5	5.15-5.16	12	In what ways does an Executive Information System differ from the Traditional Information System?

Nov-02	[7(c)]	5	5.2	5	Write short note : Decision Support Systems
Nov-03	[7(a)]	5	5.15-5.16	4	Write Short Note : Executive Information Systems
Nov-04	[2(c)]	5	5.13 - 5.14	5	Successful executives take decisions relying more on intuition than on any quantitative analytical decision technique. Mention five characteristics of the types of information that are responsible for this phenomenon in executive decision-making.
May-05	[2(b)]	5	5.2-5.5	5	"A decision support system supports the human decision-making process rather than providing a means to replace it". Justify the above statement by stating the characteristics of decision support system.
Nov-05	[3(a)]	5	5.15-5.16	10	What is an Executive Information System? Discuss its various purposes.
May-06	[3(b)]	5	5.7-5.10	5	Describe various software tools used in Decision support system.
May-07	[3(b)]	5	5.10-5.11	10	"Decision support systems are widely used as part of an Organisation's Accounting Information system". Give examples to support this statements.
Nov-07	[6(c)]	5	5.17-5.18	5	Briefly explain the principles to guide the design of measures and indicators to be included in EIS.
May-08	[4(b)]	5	5.5-5.7	5	Briefly discuss four basic components of Decision Support System.
Nov-08	[5(a)]	5	5.15-5.16	5	What is Executive Information System (EIS)? How does EIS differ from Traditional Information Systems?

Chapter VI: *ENABLING TECHNOLOGIES*

1. What is client - server? Describe the various characteristics that reflect the features of a client - server system.

A simple definition of client/server computing is that server software accepts requests for data from client software and returns the results to the client.

Characteristics:

There are ten characteristics that reflect the key features of a client-server system. These ten characteristics are as follows:

1. Client-server architecture consists of a client process and a server process that can be distinguished from each other.
2. The client portion and the server portions can operate on separate computer platforms.
3. Either the client platform or the server platform can be upgraded without having to upgrade the other platform.
4. The server is able to service multiple clients concurrently; in some client/server systems, clients can access multiple servers.
5. The client-server system includes some sort of networking capability.
6. A significant portion of the application logic resides at the client end.
7. Action is usually initiated at the client end, not the server end.
8. A user-friendly graphical user interface (GUI) generally resides at the client end.
9. A structured query language (SQL) capability is characteristic of the majority of client-server systems.
10. The database server should provide data protection and security.

2. Benefits of the Client/Server Technology :

- Increased Productivity
- End user productivity
- Developer productivity
- Users are more productive today because they have easy access to data and because applications can be divided among many different users so efficiency is at its highest.
- Client/server applications make organisations more effective by allowing them to port applications simply and efficiently.
- The expenses of hardware and network in the client/server environment are less than those in the mainframe environment.
- Long term cost benefits for development and support.
- Reduce the cost of the client's computer disk space.
- Reduce the cost of purchasing, installing, and upgrading software programs and applications on each client's machine; delivery and maintenance would be from one central point, the server.
- Reduce the total cost of ownership.
- Easy to add new hardware to support new systems such as document imaging and video teleconferencing which would not be feasible or cost efficient in a mainframe environment.
- Takes less people to maintain a client/server application than a mainframe
- The management control over the organisation would be increased.
- Leads to new technology and the move to rapid application development such as object oriented technology.
- Can implement multiple vendor software tools for each application.

3. Components of Client - Server Architecture

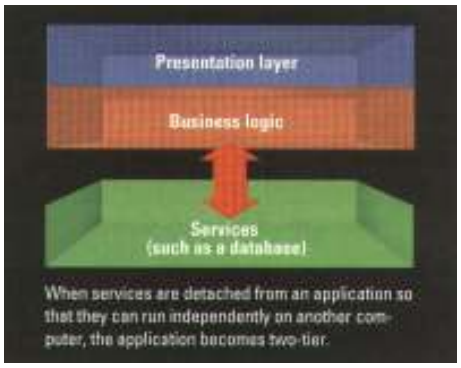
a) Client: The client is a single PC or workstation associated with software that could provide a graphical interface to server computing resources. There are basically two types of clients:
i) GUI where presentation usually is provided by visually enhanced processing software known as a Graphical User Interface (GUI). Object Oriented User Interface (OOUI) clients take GUI clients even further with expanded visual formats, multiple workplaces and object interaction rather than application interaction.
ii) Non GUI, that require minimum human intervention – includes ATMs, cell phones, Fax machines

b) Server: Server awaits requests from clients and regulates access to shared resources
File server: is a computer responsible for the central storage and management of data files so that other computers on the same network can access the files
Database server: executes SQL requests from clients
Transaction server: executes a series of SQL commands
Web servers: allow clients and servers to communicate with a universal language called HTTP
Multiple functions may be supported by a single server.

c) Middleware: Term used to describe a unique class of software employed by client-server applications. This software resides between an application and the network, and manages the interaction between the GUI on the front end and data servers on the back end. General middleware allows for communication, directory services, queuing, distributed file sharing and printing. The middleware is typically composed of four layers, which are, Service, Back-end processing, Network Operating System and Transport Stacks. E.g. Oracle's SQL*Net

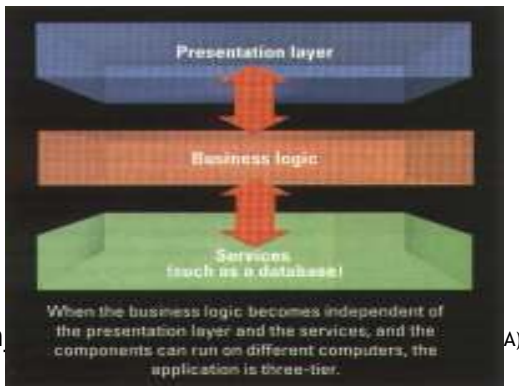
d) Two Tier/ Three Tier Server Architecture

Two Tier (Fat Client): A two-tier client server architecture defines just two parts:



1. A client, which includes a front-end program (developed using popular tools like Visual Basic, Power-Builder, Delphi or a similar program. The front-end program is in charge of two types of tasks: those related to the GUI (graphical user interface) and those related to business rules and application logic (data validation, computations, decisions, etc)
2. A database server or back end.

Three tier (Fat Server):



1. A thin client, focused on doing GUI tasks(could be an Internet browser)
2. A group (one or more) of application servers, focused on running the application logic, These servers could run programs generated in JAVA (called servlets) or with other development tools.

3. A group (one or more) of database servers.

e) Network : The network hardware is the cabling, the communication cords and the device that link the server and the clients.

4. Client - Server risk and issues:

1. Technological Risks: Will the new system work? How soon will it become obsolete?
2. Operational Risks: Will you achieve the performance you need. Software that you chose is able to grow or adapt to the changing needs of the business.
3. Economic Risks: In the long run, the concern centers around the support costs of the new system.
4. Political Risks: Will end users and management be satisfied.

5. Client - Server Security:

Security procedures are not clearly defined or protected, as they utilise distributed techniques, there is an increased risk of access to data and modification.

To increase security, the IS Auditor should ensure that the following control techniques are in place:

i. Disabling Floppy disk drive.
ii. Diskless workstations
iii. Unauthorised users may be prevented from overriding login scripts and access by securing automatic boot or startup batch files.
iv. Network monitoring
v. Data encryption techniques
vi. Authentication systems
vii. Smart cards – It uses intelligent hand held devises and encryption techniques to dechiper random access codes provided by client-server based operating systems. A smart card displays a temporary password based on an algorithm and must be re-entered by the user during the login session for access onto the client-server system
viii. Application controls

6. Server - Centric Model

Server – centric computing is a model, in which application are deployed, managed, supported and executed 100% on a server. The client handles data entry and information display.

It uses a multi-user operating system and a method of distributing the presentation of an application's interface to a client device. With server based computing, client devices, whether "fat" or "thin", have instant access to business-critical application via the server – without application rewrites or download. This means improved efficiency when deploying business-critical applications. In addition, server-based computing works within the current computing infrastructure and current computing standards, and with the current and future family of windows-based offering to improve returns on computing investments-desktops, networks, applications and training. As the result, server-based computing is rapidly becoming the most reliable way to reduce the complexity and total costs associated with enterprise computing.

Recently expanded model now includes web-based application where users browse through data over the network. Almost any client device can be adapted for the use with server-centric application. Whether the user is using traditional terminals, GUI/Windows terminals, network computers, or personal computers, the overall solution's performance depends primarily on network bandwidth and the number of user connecting simultaneously. The more users accessing the server resources, the slower the response time.

While other approaches for deploying, managing and supporting business-critical applications across the expanded enterprise have been introduced, only the server based computing model provides today growing enterprises with the tools and capabilities they need to be successful.

Year of Exam	Question No.	Chapter No.	Ans. Page No.	Marks	Question
Nov-02	[3(a)]	6	6.9	8	Explain the major categories of risks involved from the mainframe Computers to client servers?
May-03	[6(b)]	6	6.3, 6.5	10	What is client/ server? Describe the various characteristics that reflect the features of a client/ server/ server system.
Nov-03	[3(a)]	6	6.7-6.8	8	Describe the various components of Client-Server architecture
May-04	[5(c)]	6	6.3, 6.4	12	What is client/ server technology? Enumerate any six of its benefits.
Nov-04	[3(c)]	6	6.9	10	Describe four categories of risks that are to be considered during the transaction from the mainframe (or PC) to client/server.
Nov-04	[3(b)]	6	6.8	8	What are the control techniques to be checked to ensure security for client/ server technology?
Nov-04	[3(a)]	6	6.7 - 6.8	2	Define a 2-tier and 3-tier architecture.
May-05	[7(c)]	6	6.3	5	Write short notes on: Client-server model
Nov-05	[7(a)]	6	6.10-6.11	5	Server - centric model
May-06	[3(c)]	6	6.7-6.8	5	Describe various components of clients server architecture.
May-07	[6(b)]	6	6.8	5	What are control techniques that are essential for the security of the client/server environment?
May-08	[5(b)]	6	6.9	5	Briefly explain the risks associated with client / server model.
Nov-08	[4(b)]	6	6.8	5	What control techniques can be utilized for increasing security in a client-server model?

Chapter VII: *SYSTEM DEVELOPMENT PROCESS*

1. System Development life cycle

1. Preliminary Investigation – undertaken when users come across a problem or opportunity and submit a formal request for a new system

a) Request clarification
b) Feasibility analysis (Technical, Economic, Operational , Schedule, Legal feasibility)

2. Requirement Analysis Or Systems Analysis
a) Determining the user information requirements.
b) Analysis of present System.
c) System analysis of proposed system.

3. System design
Designing the user interface, files to be used, and information processing functions to be performed by the system

4. Development of Software
a) Program development
Designing, coding, compiling, testing and documenting programs.
b) Procedures and forms development
Designing and documenting systems procedures and forms for the users of the system.

5. System testing
Acceptance testing
Final testing of the system and formal approval and acceptance by management and users.

6. Implementation and Maintenance
a) Conversion
Changeover from the old system to the new system
b) Operation and maintenance
Ongoing production running of the system and subsequent modification and maintenance in light of problems detected.
The life-cycle approach **does not imply that all these phases must be carried out serially**.
Some can proceed concurrently; for example, procedures and forms development can occur at the same time program development are undertaken.

2. Reasons for failure of objectives of Systems development :

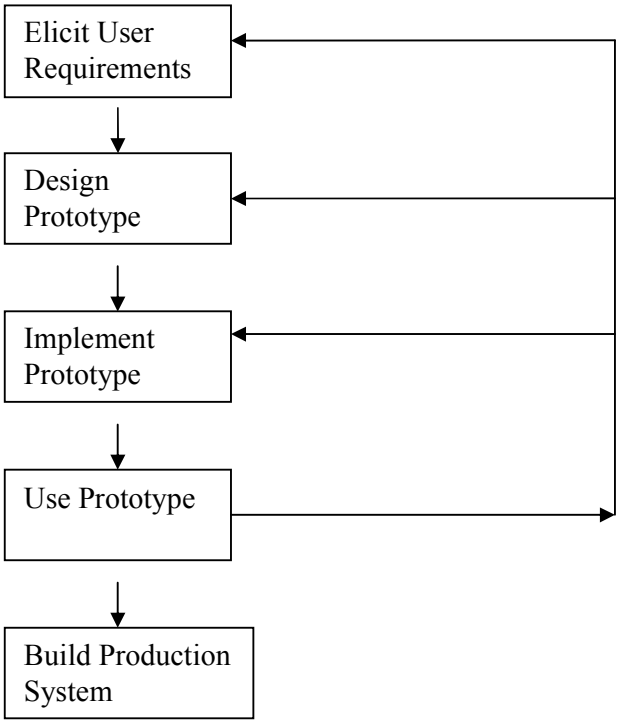
a) Lack of senior management support for and involvement in information systems development.
b) Shifting user needs
c) Development of strategic systems
d) New technologies – Personnel being not familiar with technology
e) Lack of standard project management and systems development methodologies
f) Overworked or under-trained development staff
g) Resistance to change
h) Lack of user participation
i) Inadequate testing and user training

3. Approches to SDLC.

1. *Traditional*:

(See Pt. 1)

2. *Prototyping Approach* :
The prototyping approach is founded on the assumption that resolution of requirement uncertainty is a legitimate and important task. It involves developing an initial prototype system, gaining experience, and continuing to iterate through this cycle unit an acceptable solution is found



Auditors must be concerned about whether end users always have sufficient knowledge to design and implement high quality information systems.
In general, the procedure is useful when one or more of the following conditions exist:
1. End-users do not understand their informational needs very well.
2. System requirements are hard to define.
3. The new system is mission-critical or is needed quickly.
4. Past inter actions have resulted in misunderstandings between end users and designers.
5. The risks associated with developing and implementing the wrong system are high.

Advantages:
1. Results in a better definition of these users, needs and requirements.
2. A very short time period (e.g., a week) is normally required to develop and start experimenting with property.
3. Errors are hopefully detected and eliminated early in the developmental process.

Disadvantages:
1. Functions or extras being not included in the initial requirements document.
2. Functionally rich but inefficient.
3. Finished system will have poor controls.

3. *End user development approach:* With the increasing availability of low-cost technology, end user development is becoming popular in many organisation. In end-user

development, **it is the end user and not the computer professional who is responsible for systems development activities.**

a. A decline in standards and controls.
b. Inaccuracy of specification requirements.
c. Reduction in the quality assurance and stability of the system.
d. In unrelated and incompatible systems.

4. *Top down approach:* Assumes a high degree of top management involvement in the planning process and focuses on organizational goals.

a. Analyse the objective and goals
b. Identify the functions and explain how they support the entire organisation.
c. Based on the functions identified above, ascertain the major activities, decisions and functions of the managers at various levels of hierarchy.
d. Find out the information requirements for activities and decisions.
e. Prepare specific information processing programs in detail and modules.

5. Bottom up approach: **Starts from the identification of life stream systems. Life stream systems are those systems, which are essential for the day-to-day business activities.** Ascertaining the data/information requirements files requirements and processing programs for each life stream system. Integration of data kept in different data files. Addition of decision models and various planning models for supporting the planning activities involved in management control. Models are integrated to evolve model base.

4. System Development Tools:

a. Systems flow chart: It is a graphic diagramming tool that documents and communicates the flow of data media and information processing procedures taking place at the physical or resource level in the system. It is also used to show controls exercised at the physical or resource level in the system.
b. Data flow diagrams: A data flow diagram (DFD) graphically describes the flows of data at the logical or functional level in a system. A DFD is composed of four basic elements: data source and destinations, data flows, transformation processes, and data stores.
c. Layout forms and screens: These consist of electronic displays or preprinted forms on which the size and placement of titles, heading, data and information can be designed. CASE tools and other software packages for computer-aided development of information systems provide electronic version of layout forms.
d. Systems components matrix: Can be used as an information system framework for both systems analysis and system design. It highlights how the basic activities of input, processing, output, storage and controls are accomplished and how use of hardware, software and people resources can convert data into information products.
e. CASE Tools: The data flow diagram and system flow charts that users review are commonly generated by systems developers using the on-screen drawing modules found in CASE (Computer-Aided-Software Engineering) software packages. CASE refers to the automation of any thing that humans do to develop systems. CASE products can support virtually all phases of traditional system development process.
f. Data Dictionary: A data dictionary is a computer file that contains descriptive information about the data items in the files of a business information system. Thus, a data dictionary is a computer file about data.
    I. Codes describing the data item's length (in characters), data type (alphabetic numeric, alphanumeric, etc.), and range (e.g. values from 1 to 99 for a department code)
    II. The identity of the source document(s) used to create the data item.
    III. The names of the computer files that store the data item.

IV. The names of the computer programs that modify the data item.
V. The identity of the computer programs or individuals permitted to access the data item for the purpose of file maintenance, upkeep, or inquiry.
VI. The identity of the computer programs or individuals not permitted to access the data item.

Data Dictionary serves as a documentation aid to programmers and system analysts, who study, correct, or enhance either the database or the company programs that access it. It can help establish an audit trail because it can identify the input sources of data items, the computer programs that modify particular data items, and the managerial reports on which the data items are output.

5. System Development Team:

a) Steering Committee:
This committee usually consists of a group of key IS services users that acts as a review body for IS plans and applications development. The steering committee ensures that ongoing systems development activities are consistently aimed at satisfying the information requirements of managers and users within the organisation.

b) IS Department:
It becomes the responsibility of the IS department to develop the systems.

c) Project Management:
In order to coordinate development activities of the system, a project management team generally consisting of both computer professionals and key users is appointed.

d) Systems Analysts:
System analysts are subsequently assigned to determine user requirements, design the system and assist in development and implementation activities.

In end-user developed systems, the end-user is ultimately responsible for the system.

6. Stages in SDLC:

Stage I: The Preliminary Investigation

Whatever may be the reason, managers and users may feel compelled to submit a request for a new system. The request for the project development should first be reviewed. The purpose of the preliminary investigation is to evaluate the project request.

Objectives of preliminary investigation are:
a. Clarify
b. Determine the size of the project
c. Determine the technical operational and economic feasibility
d. Cost and benefits analysis
e. Report

A Conducting Investigation:
1. Reviewing internal documents: Analysts can usually learn these details by examining organisation charts and studying written operational procedures.
2. Conducting Interviews: Interviews allow analysts to know me about the nature of the project request and the reasons for submitting.

B. Determine the Size of the project:

After problems or opportunities are identified, the analysts must determine the scale of response needed to meet the user's requests for new system as well as the approximate amount of time and money that will be required in the effort.

C. Determine the technical operational and economic feasibility:
The proposed system is evaluated from a technical view point first and if technically feasible, its impact on the organisation and staff is assessed. If a compatible technical and social system can be devised, it is then tested for economic feasibility.

(i) Technical feasibility
Does the necessary technology exist to do what is suggested (and can it be acquired)?
Does the proposed equipment have the technical capacity to hold the data required to use the new system?
Will the proposed system provide adequate responses to inquire, regardless of the number or location of users?
Can the system be expanded if developed?
Are there technical guarantees of accuracy, reliability, ease of access, and data security?

(ii) Economic feasibility
This is the most difficult aspect of the study.

(iii) Operational feasibility
It is concerned with ascertaining the views of workers, employees, customers and suppliers about the use of computer facility. The support or lack of support that the firm's employees are likely to give to the system is a critical aspect of feasibility.

(iv) Schedule feasibility
Schedule feasibility involves the design team's estimating how long it will take a new or revised system to become operational and communicating this information to the steering committee.

(v) Legal feasibility:
Legal feasibility is largely concerned with whether there will be any conflict between a newly proposed system and the organisation's legal obligations.

D. Estimating costs and benefits:
After possible solution options are identified, the analyst should make a primary estimate of each solution's costs and benefits.
Cost:
a. Development costs
b. Operational and Maintenance cost
Benefits:
a. Tangible: Tangible benefits are those that can be accurately measured and are directly related to the introduction of a new system, such as decrease in data processing cost.
b. Intangible: Intangible benefits such as improved business image are harder to measure and define.
Intangible though it its important to put a rupee and paise tag to each benefit for purposes of profit and loss statement, which can be done with diligence on the part of operating managers.

E. Reporting Results to Management:
The report should be accompanied by a short cover letter that summarizes the result and makes the recommendation regarding further procedures.

STAGE II: <u>Requirements Analysis/System Analysis</u>:

The focus is on determining user needs, studying the application area in depth, assessing the strengths and weakness of the present system and reporting results to management. However, under prototype approach the requirement analysis and design phases proceed in tandem and in small increments. How thoroughly the present system is studied depends on the situation.

A. Fact finding techniques:
To assess these needs, the analysts often, interact extensively with the people, who will be benefited from the system, in order to determine what are their actual requirements.

1. Documents : Document means manuals, input forms, diagrams of how the current system works, associated with the current system etc. Documents are a very good source of information about user needs and the current system.

2. Questionnaires: Large amount of data can be collected through a variety of users quickly. Also, if the questionnaire is skillfully drafted, responses can be analysed rapidly with the help of a computer.

3. Interviews : Users and managers may also be interviewed to extract information in depth.

4. Observation : In prototyping approaches, observation plays a central role in requirement analysis. Only by observing how users react to prototypes of new system, the systems can be successfully developed. In the traditional approach, observation is not always mandatory. But it it's desirable in most instances.

B. Analysis of the Present System

1 Review historical Aspects : A brief history of the organsation identify the major turning points and milestones.

2. Analyse inputs: A detailed analysis of present inputs is important since they are basic to the manipulation of data. The system analyst must understand the nature of each form, what is completed, the distribution of the form and other similar considerations.

3. Review data files maintained : The analyst should investigate the data files maintained by each department, noting their number and size, where they are located, who uses them and the number of times per given time t\interval these are used.

4. Review methods, procedures and data communications : A method is defined as a way of doing something; a procedure is a series of logical steps by which a job is accomplished. A system analyst also needs to review and understand the present data communications used by the organisation.

5. Analyse outputs : The outputs or reports should be scrutinized carefully by the system analysts in order to determine how well they will meet the organisation's needs.

6. Review internal controls : Locating the control points helps the analyst to visualize the essential parts and framework of a system.

7. Model the existing physical system and logical system : The logical flow of the present information system may be depicted with the help of system flow charts. The physical flow of the existing system may be shown by employing data flow diagrams.

8. Undertake overall analysis of present system :

C System Analysis of Proposed Systems :
After each function area of the present information system has been carefully analysed, the proposed system specifications must be clearly defined. The required systems specifications which should be in conformity with the project's objectives are as follows:

a. Outputs produced with great emphasis on timely managerial reports that utilise the "management by exception" principle.
b. Database maintained with great accent on online processing capabilities.
c. Input data prepared directly from original source documents for processing by the computer system.
d. Methods and procedures that show the relationship of inputs and outputs to the database, utilizing data communications where deemed appropriate.
e. Work volumes and timings carefully considered for present and future periods including peak periods.

The starting point for compiling these specifications is output. After outputs have been determined, it is possible to infer what inputs, database, methods, procedures and data communications must be employed.

Year of Exam	Question No.	Chapter No.	Ans. Page No.	Marks	Question
Nov-02	[3(b)]	7	7.8-7.9	8	Describe the steps involved in prototyping for Systems development.
Nov-02	[7(a)]	7	7.39 - 7.40	5	Write short note : Data Dictionary
Nov-02	[3(c)]	7	7.9-7.10	4	If you are the Project Manager of a Software Company with the responsibility for developing a break-through product, combining state of the art hardware and software, will you opt for prototyping as a process model for a product meant for the intensely competitive entertainment market?
May-03	[3(a)]	7	7.29	10	Describe briefly four categories of the major tools that are used for system development.
Nov-03	[3(b)]	7	7.5-7.6	12	Bring out the reasons as to why the organizations fail to achieve their Systems Development Objectives?
May-04	[2(b)]	7	7.8-7.9	8	Discuss the four steps of the prototyping approach in system development
May-04	[2(a)]	7	7.2-7.4	2	What is a system development Life-cycle?
Nov-04	[7(d)]	7	7.2 - 7.4	5	Write short note: System Development Life-cycle.
May-05	[4(b)]	7	7.25-7.27	5	Describe any five functional areas of a system which needs to be analyzed by system analyst for detailed investigation of the present system.
May-05	[7(b)]	7	7.39	5	Write short notes on: Data dictionary
Nov-05	[6(a)]	7	7.22-7.23	10	What are the various Tangible and Intangible benefits that can result from the development of a computerised system ?
Nov-05	[2(c)]	7	7.24-7.25	5	What are the fact finding techniques used by a system analyst?
May-06	[3(a)]	7	7.25-7.27	10	A company is offering a wide range of products and services to its customers. It relies heavily on its existing information system to provide up to date information. The company wishes to enhance its existing systems. You being an Information System auditor, suggest how the investigation of the present information system should be conducted so that it can be further

					improved upon.
May-06	[7](ii)	7	7.11	5	Write Shot notes on any four of the following: (ii) Top down approach of system development.
Nov-06	[3(a)]	7	7.13-7.14	10	What are the project management items associated with an I.T. project system failures? Give the elements to be included in the adopted framework to avoid such failures.
May-07	[5(a)]	7	7.7-7.10	10	What is prototyping approaches to systems development? Describe its advantages and disadvantages also.
May-07	[7(a)]	7	7.39-7.40	5	Data dictionary
Nov-07	[1(d)]	7	7.24-7.25	5	Briefly explain the various fact finding techniques which are used by the system analyst for determining the needs of an organization.
Nov-07	[4(b)]	7	7.2-7.4	5	Discuss the various activities which are part of the system development life cycle.
Nov-07	[7(d)]	7	7.10-7.11	5	End user development approach in system development
May-08	[3(a)]	7	7.25-7.27	10	Discuss in detail, how the investigation of present system is conducted by the system analyst.
Nov-08	[2(b)]	7	7.28-7.29	10	State main objectives of system development tools. Briefly describe the major categories of documentation tools that are used for system development with any one simple illustrative example for each.

Chapter VIII: *SYSTEMS DESIGN*

1. Systems Design

The system design phase usually consists of following three activities:

a) Reviewing the system's informational and functional requirements must conform to the purpose, scale and general concepts of the system that management approved.

b) Developing a model of the new system, including logical and physical specifications of outputs, inputs, processing, storage, procedures and personnel - System design involves first logical design and then physical construction of a system. Physical construction, the activity following logical design produces program software, files and a working system.

c) Reporting results to management.

The logical design of an information system is like an engineering blueprint; it shows major features of the system and how they are related to one another.

2. Areas to be concentrated on for design a model for new system

1. Output

a) Objective: Convey required information, Signal important event, Trigger action and confirmation of action.

b) Important factors:

i. Content: Too much content can cause managers to waste time in isolating the information that they need; it also diminishes the impact of truly important information. Hence, only the required information should be included in various outputs.

ii. Form: Form refers to the way that content is presented to users. Content can be presented in various forms; quantitative, non-quantitative, text, graphics, video and audio.

iii. Output volume: The amount of data output required at any one time is known as output volume.

iv. Timeliness: Timeliness refers to when users need outputs.

v. Media: Refers to physical device where the output will be displayed vi2
paper, video display, etc.

vi. Format: The manner in which data are physically arranged is referred to as format. The real issue in designing computer output is not how much can be provided, but how little is needed to make important information available.

c) Presentation:

i. Tabular Format: Routine reports, summarises

ii. Graphic Format: Top level management presentations.

d) Designing printed output:
Guidelines:

i. Documents should be designed to read from left to right and top to bottom.

ii. Most important items should be easier to find.

iii. Heading or title of the report, page number, date of preparation and column headings.

iv. Attention should be drawn to control breaks summaries and other important information by boxing them off with special characters.

v. Sufficient margin

e) Designing visual display output:
Attention should be paid to

i. Physical dimensions of the screen

ii. Degree of resolution (high, medium, low);

iii. Colours available

iv. Methods of highlighting

v. Methods of intensity control

vi. No. of Rows and Columns that can be displayed

2. Designing systems inputs:

a) Important factors

i. Content: To consider the types of data that are needed to be gathered to generate the desired user outputs.

ii. Timeliness: A plan must be established regarding when different types of inputs will enter the system.

iii. Media: Includes the choice of input media and subsequently the devices on which to enter the data.

iv. Format: Refers to the format of records viz. type and length of records.

v. Input volume: Amount of data to be entered.

b) Capturing data effectively by well-designed input forms and visual display terminals.
Considerations for Form design

i) Easy to fill forms with proper form flow, logical sections, and captioning.

ii) Meeting the intended purpose

iii) Ensuring accurate completion with the help of data validation procedure and progress.

iv) Keeping forms attractive.

v) Coding methods:

a) Characteristics of good coding scheme:

i. Individuality: The code must identify each object in a set uniquely and with absolute precision.

ii. Space: Much briefer than description.

iii. Convenience: Should facilitate their use by people.

iv. Expandability: Future growth in the number of objects in a set should be provided for.

v. Suggestiveness: The letter or number should be suggestive of the item characteristics.

vi. Permanence: Changing circumstances should not invalidate the scheme.

b) Coding Schemes:

i. Classification codes: Classification codes place separate entities, such as events, people, or objects into distinct groups called classes. For example, a passenger car traveling the bridge is categorised as class 1 vehicle and charged, a two wheeler trailer is coded as class 2, four wheeler trailer is classified as class 3.

ii. Function codes: Function codes state the activities or work to be performed without spelling out all of the details in narrative statements.

iii. Significant-digit subset codes: Codes can be divided into subsets or subcodes. The subcodes give the user additional information about the item.

iv. Mnemonic codes: These are suitable where the codes have to be remembered by people.

v. Hierarchical Classification.

3. Data Storage

Approach I:

The first approach is to store data in individual files, one file for each application.

Approach II:

The second approach is to develop a data base that can be shared by many users for a variety of applications as need arises preferred when data needs to be centrally located as it is to be used by users spread over geog distances, and required in multiple applications.

Although systems analysts do not design database, a separate database management staff oversees the design and development of the database. However, the analyst must work with data

base administrators to determine how data will be stored and what methods will be used for their retrieval and conversion to the format the program requires.

4. Data Communications

The systems analyst is responsible not only for selecting the right communication equipment, whether it is for large or small systems or whether transmission is over wide or limited areas, but also for the steps that must be taken to design the application, specifying the method for linking the application into the communication network and selecting the most useful and cost effective communication services.

The system analysts must select the following components:

1. For communications channels, he may have to make a decision regarding channel selection, transmission rate, leased or dial-up line, type of line, for example, simplex or half-duplex etc.
2. Communications control devices: The analyst is required to select devices such as modems, data service units, multiplexer and concentrator, data switches, etc. In addition the analyst may also select the type of network (LAN or WAN), network topology (point-to-point or multi drop) etc. and the network architecture to be utilized for the proposed project.

5. System Manual

The output of the system design exercise is a description of the task to be performed, complete with layouts and flowcharts. This is called the job specifications manual or system manual. It contains:

i. General description of the existing system
ii. Flow of the existing system
iii. Outputs of the existing system
iv. General description of the new system
v. Flow of the new system
vi. Output layouts
vii. Output distribution
viii. Input layouts
ix. Input responsibility
x. Macro-logic-The overall logic of the internal flows
xi. Files to be maintained
xii. List of programs
xiii. Timing estimates
xiv. Controls
xv. Audit trail
xvi. Glossary of terms used.

6. Reporting to management

The report should include

1. description of the application and users source that led to the system
2. a summary of the results of the requirement analysis
3. design recommendation.
4. any changes in the costs and benefits of the new system.
5. a plan for the remaining system development activities.

Year of Exam	Question No.	Chapter No.	Ans. Page No.	Marks	Question

Nov-02	[6(b)]	8	8.14-8.15	10	What are the major factors to be considered in designing User inputs? Explain.
Nov-03	[7(b)]	8	8.26-8.27	4	Write Short Note : System Manual
May-04	[3(a)]	8	8.3-8.4	10	What are the six important factors which should be considered while designing the user outputs?
May-05	[3(a)]	8	8.3-8.4	10	What are the factors considered to design the ideal layout of a printed output?
May-05	[5(c)]	8	8.18-8.19	5	Discuss the desired characteristics of a good coding system.
Nov-05	[3(b)]	8	8.14-8.15	10	Discuss various issues that should be considered while designing system input.
May-06	[6(c)]	8	8.15-8.18	5	Suggest suitable guidelines to be followed for efficient form design.
Nov-06	[3(b)]	8	8.19-8.22	5	Discuss some of the commonly used coding schemes.
May-07	[4(a)]	8	8.26-8.27	10	What is system manual? What information is included in it?
Nov-07	[4(c)]	8	8.8-8.9	5	State the standards to be followed while designing graphical output
May-08	[5(a)]	8	8.14-8.15	5	Discuss various issues that should be considered while designing system input.
Nov-08	[4(c)]	8	8.18-8.19	5	What are the characteristics of good coding scheme for data input?

Chapter IX: *SYSTEM'S ACQUISITION, SOFTWARE DEVELOPMENT AND TESTING*

1. Acquiring systems components from vendors
   The system development team often prepares a list of specific needs. Management also decides whether the hardware is to be purchased, leased from a third party or to be rented.
   Following points to be considered:
   1. The latest possible technology should be acquired.
   2. Computer performance for commercial work is mainly determined by **the speeds and capabilities of input/output and storage peripherals**. Scientific, engineering and operations problems require good computational facilities.
   3. Experts maintain that since hardware speed and facilities are uniformly good, **today the selection of computer should be made on software considerations**. Manufacturers also offer packages specially designed for a particular industry such as packages for airline reservations and packages of application in banking and insurance.
   4. The choice of a computer really becomes **a choice of a model computers are marketed as series of compatible machines** with increasingly powerful central processors and interchangeable peripherals within a series, based on a long-range plan of expansion.
   5. Outside assistance in computer selection can be had from computer manufacturers. The distinction between vendor selection and machine selection is to be carefully noted at this stage. **Choosing the vendor is essentially a matter of business judgment and prerogative of exercising it must be retained in-house.**
2. Software Acquisition: Make or Buy
   At this stage, the system developers must determine whether the application software should be created in-house or acquired from a vendor. This decision is often called the make-or-buy decision.
   Advantages of Application Packages:
   i. Rapid implementation:
   ii. Low risk: Package is available in the finished form, the organisation knows what it is going to get for the price it has paid.
   iii. Quality: The firms engaged in application package developments are typically specialist in their products' niche area.
   iv. Cost: An application package generally costs less than an in-house developed package. Vendors can leverage the cost of developing a product by selling the product to several other firms.
3. Steps involved in selection of a computer system
   1. Prepare the design specifications
   2. Prepare and distribute an RFP (Request for proposal) to selected computer vendors. Typically, the RFP also contains a deadline for bidding.
   3. On the basis of an analysis of proposals, eliminate vendors whose proposals are inferior.
   4. Have vendor present their proposals.
   5. Conduct further analysis of the proposals.
   6. Contact present users of the proposal systems.
   7. Conduct equipment benchmark tests.
   8. Select the equipment.
4. Validation of vendors' proposals
   a) Factors
   1. The performance Capability of Each Proposed System in Relation to its Costs
   2. The Costs and Benefits of Each Proposed System
   3. The Maintainability of Each Proposed System
   4. The Compatibility of Each Proposed system with Existing System
   5. Vendor Support

a. training classes
b. help in implementing and testing the new system
c. assistance in maintaining the new system

b) Methods

1. Checklists: It is the most simple and rather a subjective method for validation and evaluation. The various criteria are put in checklist in the form of suitable question against which the responses of the various vendors are validated.
2. Point-Scoring Analysis: When performing a point scoring analysis, the evaluation committee first assigns potential points to each of the evaluation criteria based on its relative importance. After developing these selection criteria, the evaluation committee proceeds to rate each vendor or package, awarding points, as it deems fit. The highest point total determines the winner.
3. Public evaluation reports: Several consultancy agencies compare and contrast the hardware and software performance for various manufacturers and publish their reports in this regards. This method is particularly useful where the buying staff has inadequate knowledge of computer facts.

5. Software Development
   1. Program analysis: Ascertains for a particular application the outputs required the inputs available and the processing then determines whether the proposed application can be or should be programmed at all.
   2. Program design: In this stage the programmer develops the general organisation of the program as it relates to the main functions to be performed.
   3. Program coding: The logic of the program outlined in the flowcharts is converted into program statements or instructions at this stage. Different programmers may write a program using different sets of instructions but each giving the same results. Therefor, the programmers broadly pursue three objectives; simplicity, efficient utilisation of storage and least processing time.
   4. Debug: The process of debugging a program refers to correcting programming language syntax and diagnostic errors so that the program "compiles cleanly".
   5. Program documentation: The writing of narrative procedures and instructions for people who will use software is done throughout the program life cycle. User documentation should also be reviewed for understandability.
   6. Program maintenance: The requirements of business data processing applications are subject to continual change. This calls for modification of the various programs.

6. Program Design Tools
   1. Program flow chart: Program flow chart is among the most common progress design tools. These flow charts depict the logical steps through which a computer program must proceed when solving a problem.
   2. Pseudo code: Pseudocode like program flow charts, also represents program logic. However, instead of using graphical symbols and flow lines, **pseudo code presents program logic in English-like statements.**
   3. Structure chart: The structure chart organises each of the program tasks into well-defined modules. The higher-level modules represent control portions of the program; the lowest level modules do the actual task of the program.
   4. 4GL Tools: The main drawback of manually applied tools - lot of time to prepare. Not sure if it is internally consistent. 4GL Tools automate many of the tasks done manually. The automation of tasks and internal consistency checks are the two reasons due to which productivity gains result from using 4GL tools. All 4GLs are designed to reduce prog. Effort, the time it takes to develop software and the cost of software development.

5. Object oriented programming and design tools: Object oriented software design results in a model that describes object, classes and their relationships to one another. For example Microsoft's Application
   a. tools for creating and manipulating objects
   b. a visual programming environment for constructing object and application interfaces
   c. a shell that supports either object oriented programming or traditional structured program.

7. System Testing

   System-level testing must be conducted prior to installation of an information system.
   a. preparation of realistic test data.
   b. processing the test data
   c. thorough checking of the results
   d. reviewing the results with future users

   System level testing is an excellent time for training employees. One of the most effective ways to perform system-level testing is to perform parallel operations with the existing system. Parallel operations consist of feeding both systems the same input data and comparing data files and output results. During parallel operations, the mistakes detected are often not those of the new system, but of the old. These differences should be reconciled as far as it is feasible economically.

Year of Exam	Question No.	Chapter No.	Ans. Page No.	Marks	Question
May-03	[4(a)(ii)]	9	9.4	4	Enumerate the advantages of prewritten application software packages.
May-03	[4(a)(iii)]	9	9.3-9.4	4	Discuss the factors upon which "Make or Buy" decision of application software depends.
May-03	[4(a)(i)]	9	9.4	2	What is application software?
Nov-03	[7(d)]	9	9.10-9.11	4	Write Short Note : Point Scoring analysis in Vendor Evaluation
May-04	[3(b)]	9	9.18-9.21	10	Describe any five program design tools.
Nov-04	[4(a)]	9	9.4 - 9.5	5	List the various sources of acquiring the software.
Nov-04	[4(b)]	9	9.4	5	Discuss four most compelling advantages of using a pre-written application package.
May-05	[3(b)]	9	9.6-9.7	10	What is Vendor evaluation? Define the process for the same.
Nov-05	[4(a)]	9	9.13-9.18	10	Discuss various stages through which an in-house creation of program has to pass.
Nov-05	[6(b)]	9	9.4	5	What are the advantages of using pre-written application packages?
May-06	[4(b)]	9	9.6-9.7	5	Briefly discuss about various factors which should be considered for evaluating the vendor proposal for supply of computer system.
May-06	[7](v)	9	9.4-9.5	5	Write Shot notes on any four of the following: (v) Sources pf packaged software
Nov-06	[3(c)]	9	9.12-9.13	5	Discuss Bench marking problem on vendor's proposal.
Nov-07	[5(a)]	9	9.18-9.21	10	Briefly discuss any five program design tools.
May-07	[2(a)]	9	9.13-9.18	10	State and briefly explain the various stages of developing an in-house program.

Nov-07	[6(b)]	9	9.5	5	State the steps involved in selection of computer systems.
May-08	[5(d)]	9	9.21-9.22	5	Briefly describe various steps involved in system testing.
May-08	[7(c)]	9	9.16-9.17	5	Write short note: Program documentation.
Nov-08	[4(a)]	9	9.2-9.3, 9.11	10	Discuss in brief salient features of consideration while selecting a computer system. Also suggest contents in a point scoring table for evaluation of a ready to use software.

Chapter X: *SYSTEMS IMPLEMENTATION AND MAINTENANCE*

1. Equipment Installation

   Steps

   a. Site Preparation: It is very important to lay down proper procedures for acquiring and planning space layout in the systems implementation. A bad layout can not only drastically reduce the productivity of the data processing department but also that of the entire organisation as whole. The electric lines should be checked to insure that they are free of static or power fluctuation. It will be better to install a 'clean' line that is not shared by other equipments. Rough layout, make cost estimates and get them approved from top management carpets etc should be avoided since they create a static charge. Highly waxed floors produce same effect. Better to have site pre-completed prior to delivery.

   b. Equipment installation: The equipment must be physically installed by manufacturer, connected-to the power source and wired to communication lines required.

   c. Equipment checks out: The equipment must be turned on for testing under normal operating conditions. Not only the routine 'diagnostic test' should be run by the vendor, but also the implementation team should devise and run extensive test of its own to ensure that equipments are in proper working condition.

2. Training Personnel

   a. Training Systems Operators: Many systems depend on the computer-center personnel, who are responsible for keeping the equipment running as well as for providing the necessary support services. As part of their training, operators should be given both a trouble shooting list that identifies possible problems and remedies for them, as well as the names and telephone numbers of individuals to contact when unexpected or unusual problem arise.

   b. User training: Most user training deals with the operation of the system itself. Users should be trained on data handling activities such as editing data, formulating inquires and deleting records of data. Many managers have to release employees from their regular job activities so that they can be trained.

3. Conversion Or Changeover From Manual To Computersised System: Conversion or changeover is the process of changing from the old system (manual system) to the new system.

   a. Direct Changeover: Conversion by direct changeover means that on a specified date., the old system is dropped and the new system is put into use. Direct changeover can only be successful if extensive testing is done beforehand. Direct changeover is considered a risky approach to conversion, and disadvantages are numerous.

   b. Parallel conversion: This refers to running the old system and the new system at the same time, in parallel. Both systems are run simultaneously for a specified period of time and the reliability of results is examined.

   The advantage: Possibility of checking new data against old data in order to catch any errors in processing in the new system. Offers a feeling of security to users.

   The disadvantage: The cost of running two systems at the same time, the burden on employees. Outputs from the systems should differ Employees who are faced, with a choice between two systems will continue using the old one because of their familiarity with it.

   c. Gradual conversion: The volume of transactions is gradually increased as the system is phased in.

   The advantage: Allowing users to get involved with the system gradually and the possibility of detecting and recovering from the errors without a lot of downtime.

   The disadvantage: Gradual conversion include taking too long to get the new system in place and its inappropriateness for conversion of small, uncomplicated systems.

d. Modular prototype conversion: Conversion uses the building of modular operational prototypes to change from old systems to new in a gradual manner.

e. Distributed conversion: One entire conversion is done at one site. When that conversion is successfully completed, other conversions are done for other sites.

The advantage: Problems can be detected

The disadvantage: Even when one conversion is successful, each site will have its own peculiarities to work through and these must be handled.

3. Activities involved in conversion

a. Procedure conversion: Operating procedures should be completely documented for the new system. This applies to both computer-operations and functional area operations. Written operating procedures must be supplemented by oral communication during the training sessions on the system change. Once the new system is completely operational, the system implementation group should spend several days checking with all supervisory personnel about their respective areas.

b. File conversion: Because large files of information must be converted from one medium to another, this phase should be started long before programming and testing are completed. In order for the conversion to be as accurate as possible, file conversion programs must be thoroughly tested. Adequate control, such as record counts and control totals, should be required output of the conversion program. The existing computer files should be kept for a period of time until sufficient files are accumulated for back up.

c. System conversion: After on-line and off-line files have been converted and the reliability of the new system has been confirmed for a functional area, daily processing can be shifted from the existing information system to the new one. A cut-off point is established so that database and other data requirements can be updated to the cut-off point. All transactions initiated after this time are processed on the new system.

d. Alternative plans in case of equipment failure: Alternative processing plans must be implemented in case of equipment failure. Priorities must be given to those jobs critical to an organisation, such as billing, payroll and inventory. Critical jobs can be performed manually until the equipment is set right. Documentation of alternative plans is the responsibility of the computer section and should be fully covered by the organisation's systems and procedures manual. It should state explicitly what the critical jobs are, how they are to be handled in case of equipment failure, where compatible equipment is located, who will be responsible for each area during downtime and what dead-lines must be met during the emergency.

4. Evaluation of the New System

a. Development evaluation: Evaluation of the development process is primarily concerned with whether the system was developed on schedule and within budget. It may be noted that very few information systems have been developed on schedule and within budget. Information systems are developed without clearly defined schedules or budgets.

b. Operation evaluation: Whether the hardware, software and personnel are capable to perform their duties and they do actually perform them so.

1. Are all transactions processed on time?
2. Are all values computed accurately?
3. Is the system easy to work with and understand?
4. Is terminal response time within acceptable limits?
5. Are reports processed on time?
6. Is there adequate storage capacity for data?

Operation evaluation is relatively straightforward if evaluation criteria are established in advance.

c. Information evaluation: An information system should also be evaluated in terms of information it provides. Therefore, the extent to which information provided by the system is supportive to decision making is the area of concern in evaluating the system. However, it is practically impossible to directly evaluate an information system's support for decision making

in an organisation. It must be measured indirectly. It is measured in terms of satisfaction user derives when his information needs are met by the system or the dissatisfaction when his information needs are not met.

6. Systems Maintenance

Most information systems require at least some modification after development. The changing organisational requirements continue to impact most information systems as long as they are in operation.

Maintenance can be categorised in the following two ways:

1. Scheduled maintenance is anticipated and can be planned for. For example, the implementation of a new inventory coding scheme can be planned in advance.
2. Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate solution. A system that is properly developed and tested should have few occasions of rescue maintenance.

An information system may remain in an operational and maintenance mode for several years.

Year of Exam	Question No.	Chapter No.	Ans. Page No.	Marks	Question
Nov-02	[7(d)]	10	10.10-10.11	5	Write short note : System Maintenance
May-03	[5(a)]	10	10.2-10.3	10	Why is personnel training important for the successful implementation of information system? What type of training should be imparted to (i) systems operator and (ii) users
Nov-03	[4(a)]	10	10.4-10.5	5	Explain the different conversion strategies used for conversion from a manual to a computerized system.
Nov-03	[4(b)]	10	10.4	3	Discuss briefly the advantages and disadvantages of any one conversion strategy.
Nov-04	[4(c)]	10	10.9 - 10.10	10	"The final step of the system implementation is its evaluation." What functions are being served by the system evaluation? Discuss development, operation and information evaluations.
May-05	[5(b)]	10	10.5-10.8	5	Explain different activities involved in conversion from manual system to computerized system.
Nov-05	[7(d)]	10	10.10-10.11	5	System maintenance
May-06	[4(c)]	10	10.4-10.5	5	Describe various strategies for change over from manual system to computerised.
Nov-06	[4(b)]	10	10.2-10.3	5	Why is personnel training important? What type of training should be imparted to users?
May-07	[6(a)]	10	10.1-10.2	10	Describe various steps that should be taken for successful installation of the equipment during the implementation phase.
May-07	[7(b)]	10	10.10-10.11	5	System maintenance
Nov-07	[4(a)]	10	10.5-10.9	10	Explain briefly various activities that should be completed for successful conversion of an existing system to the new information system.

May-08	[6(b)]	10	10.9-10.10	5	What is the purpose of the system evaluation? How is it performed?
Nov-08	[5(b)]	10	10.10-10.11	5	Define and differentiate between 'Scheduled maintenance' and 'Rescue maintenance' along with their respective benefits.

Chapter XI: *DESIGN OF COMPUTERISED COMMERCIAL APPLICATIONS*

QUESTIONS

Year of Exam	Question No.	Chapter No.	Ans. Page No.	Marks	Question
Nov-02	[4(b)]	11	11.46	6	Draw a system flow chart for a Production Scheduling system.
Nov-02	[4(c)]	11	11.46-11.47	4	What systems interfaces are involved in Production Planning?
May-03	[5(b)]	11	11.16-11.19	10	Draw a payroll flow chart explaining the processes involved.
Nov-03	[4(c)]	11	11.36,11.37,11.38	12	For a material inventory control system, draw the system flowchart and explain the following: System interfaces, Files and inputs, Reports
Nov-04	[5(b)]	11	11.32 - 11.33	5	What do your understand by ON-LINE, REAL-TIME SYSTEMS?
Nov-04	[5(c)]	11	11.34	5	For an On-line, Real-time sale order processing system, draw the systems flow chart.
May-06	[4(a)]	11	11.46-11.47	10	What do you mean by production scheduling? Draw the information flow diagram for design of computerized scheduling system. Also Explain: (i) System interface (ii) File inputs and (iii) Reports required for the above systems
Nov-06	[4(a)]	11	11.33-11.35	10	Describe the sequences of events which occur immediately for each transaction when controlled by the sales order entry computer programs in OLRT system.
May-07	[3(a)]	11	11.51-11.52	10	What is share accounting system? Describe briefly the input, outputs and processing steps involved in this system.
Nov-07	[3(b)]	11	11.36-11.37	10	What do you understand by Material Inventory Control System? Draw the Information flow diagram for designing computerized material inventory control system.
May-08	[2(a)]	11	11.40-11.42	10	What is work-in-process control system? Describe briefly the system interfaces, files and inputs, and reports involved in this system.
Nov-08	[2(a)]	11	11.13-11.17	10	What is Payroll accounting? Describe in brief the inputs and master file, output and system flow diagram required for it.

Chapter XII: *ENTERPRISE RESOURCE PLANNING : REDESIGNING BUSINESS*

1. What is ERP?

An Enterprise resource planning system is a fully integrated business management system covering functional areas of an enterprise like Logistics, Production, Finance, Accounting and Human Resources. It organizes and integrates operation processes and information flows to make optimum use of resources such as men, material, money and machine. In simple words, Enterprise resource planning promises one database, one application, and one user interface for the entire enterprise, where once disparate systems ruled manufacturing, distribution, finance and sales.

2. Characteristics and Features of ERP :

Characteristics:

a. Flexibility: Flexible to respond to the changing needs of an enterprise.
b. Modular & open: This means that any module can be interfaced or detached whenever required without affecting the other modules. Support multiple hardware platforms.
c. Comprehensive: Support variety of organizational functions and suitable for wide range of business organisation.
d. Beyond the Company: Support the on-line connectivity to the other business entities of the organization.
e. Best Business Practices: An ERP package imposes its own logic on a company's strategy, culture and organisation.

Features:

a. Supports strategic and business planning activities, operational planning and execution activities, creation of Materials and Resources.
b. End to end Supply chain Management to optimize the overall Demand and Supply Data.
c. Automatic introduction of the latest technologies like Electronic Fund Transfer (EFT), Electronic Data Interchange (EDI), Internet, Intranet, Video conferencing, E-Commerce etc.
d. Most business problems like material shortages, productivity enhancements, customer service, cash management, inventory problems, quality problems, prompt delivery etc.
e. Provides intelligent business tools like decision support system, Executive information system, and Data mining and easy working systems to enable better decisions.
f. Bridges info. Gap.
g. Better project management.
h. Complete integration of system not only across the department but also across group companies.

3. What is Business Process Reengineering?

BPR is the fundamental rethinking and radical redesign of processes to achieve dramatic improvement, in critical, contemporary measures of performance such as cost, quality, service and speed. Dramatic achievement means to achieve 80% or 90% reduction. Radical redesign means BPR is reinventing and not enhancing or improving. Fundamental rethinking means asking the question "why do you do what you do", thereby eliminating business process altogether if it does not add any value to the customer. There is no point in simplifying or automating a business process which does not add any value to the customer.

In a nutshell, a clean slate approach of BPR says that, "Whatever you are doing in the past is all wrong, do not get biased by it, reassemble and redesign it afresh."

4. Business Modelling :

A model consisting of core business processes or activities of the business is to be developed. This is the diagrammatic representation of Business as a large system with interconnection of sub-systems or processes that it comprises of.
Features of BM are as under:

1) Business processes
2) Comprehensive
3) Designed for all types of business.
4) Multinational
5) Business engineering
6) Client server architecture
7) Open system

5. ERP Implementation Methodology :

a) Identifying the Needs :

- Why should an ERP package be implemented?
- Will it improve profitability?
- Can the delivery times of products be reduced?
- How does it improve customer satisfaction in terms of quality, cost, delivery time and service?
- Will it help to reduce cost of products?
- How can it help to increase business turnover and at the same time reduce manpower?
- Will it be possible to reengineer the business processes?

b) Evaluating the "AS IS" situation of the business :
To understand the present situation of the business, the various functions should first be listed.

- Total time taken by the business processes.
- Number of decision points existing in the present scenario.
- Number of Department/Locations of business processes.
- The flow of information and its routing.
- The number of reporting points currently available.

c) Deciding the desired 'Would Be' situation :
The concept of 'Benchmarking' is used to see that processes achieved are the best in industry. Benchmarking is done on various factors like cost, quality, service etc. This concept enables to optimise the processes to gain overall benefits.

d) Reengineering the business process :

- Reduce the business process cycle time.
- To reduce the number of decision points to a minimum.
- Streamlining the flow of information and eliminating the unwanted flow of information.

e) Evaluation of various ERP packages :

a. Flexibility: It should be enable organizations to respond quickly by leveraging changes to their advantage, letting them concentrate on strategically expanding to address new products and markets.
b. Comprehensive: It should be applicable across all sizes, functions and industries.

c. Integrated: Functions should be integrated into a workflow of business events and processes across departments and functional areas.
d. Beyond the company: It should support and enable inter-enterprise business processes with customers, suppliers, banks, government and business partners.
e. Best business practices: Offer a choice of multiple ready-made business processes including best business practices that reflect the experiences, suggestions and requirements of leading companies across industries.
f. New technologies: It should incorporate cutting-edge and future-proof technologies and ensure inter-operability with the Internet and other emerging technologies.

f) Finalisation of the ERP package :
Finalisation of the ERP package can be done by making a comparison of critical factors through a matrix analysis.

g) Installation of Hardware and Networks :
This work is carried out in a phased manner depending on the schedule of implementation and need of the hardware components.

h) Finalising the Implementation Consultants :
- Skill set
- Industry specific experience
- Cost of hiring the consultant

i) Implementation of ERP packages :
The general steps involved in the implementation are:
- Formation of team
- Preparation of plan
- Mapping of Business Processes to package
- Gap Analysis i.e., deviation of existing processes from standard processes.
- Customisation.
- Development of user-specific reports and transactions.
- Uploading of Data from existing system
- Test runs.
- User Training
- Parallel run.
- Concurrence from user
- Migration to the new system
- User documentation
- Post-implementation support
- System monitoring and fine tuning.

SAP

What is SAP? SAP is the leading enterprise information and management package worldwide. Use of this package makes it possible to track and manage, in real-time, sales, production, finance accounting and human resources in an enterprise.

What Makes SAP different?

Traditional computer information systems used by many businesses today have been developed to accomplish some specific tasks and provide reports and analysis of events that have already taken place.

Examples are accounting general ledger systems. Occasionally, some systems operate in a "real-time" mode that is, have up to date information in them and can be used to actually control events. A typical company has many separate systems to manage different processes like production, sales and accounting. Each of these systems has its own databases and seldom passes information to one systems in a timely manner.

SAP takes a different approach. **There is only one information system in an enterprise, SAP**. All applications access common data. Real events in the business initiate transactions. Accounting is done automatically by events in sales and production. Sales can see when products can be delivered. Production schedules are driven by sales. The whole system is designed to be real-time and not historical.

SAP structure embodies what are considered the "best business practices". **A Company implementing SAP adapts its operations to it to achieve its efficiencies and power**.

The process of adapting procedures to the SAP model involves "Business Process Re-engineering" which is a logical analysis of the events and relationships that exist in an enterprise's operations.

SAP has several layers. The Basis System is the heart of the data operations and should not be evident to higher managerial users. Other customizing and implementation tools exist also. The heart of the system from a manager's viewpoint are the application modules. These modules may not all be implemented in a typical company but they are all related and are listed below.

FI Financial Accounting -- designed for automated management and external reporting of general ledger, accounts receivable, accounts payable and other sub-ledger accounts with a user defined chart of accounts. As entries are made relating to sales production and payments journal entries are automatically posted. This connection means that the "books" are designed to reflect the real situation.

CO Controlling -- represents the company's flow of cost and revenue. It is a management instrument for organizational decisions. It too is automatically updated as events occur.

AM Asset Management -- designed to manage and supervise individual aspects of fixed assets including purchase and sale of Assets, depreciation and investment management.

PS Project System -- is designed to support the planning, control and monitoring of long-term, highly complex projects with defined goals.

WF Workflow -- links the integrated SAP application modules with cross application technologies, tools and services.

IS lndustry Solutions -- combine the SAP application modules and additional industry-specific functionality. Special techniques have been developed for industries such as banking, oil and gas, pharmaceuticals, etc.

HR Human Resources -- is a complete integrated system for supporting the planning and control of personal activities.

PM Plant Maintenance -- In complex manufacturing process maintenance means more than sweeping the floors Equipment must be services and rebuilt. These tasks affect the production plans.

MM Materials Management -- supports the procurement and inventory functions occurring in day to day business operations such as purchasing, inventory management, reorder point processing, etc.

PP Production Planing -- is used to plan and control the manufacturing activities of a company. This module includes; bills of material, routines, work centers, sales and operations planning, master production scheduling, material requirements planning shop floor control, production orders, product costing etc.

SD Sales and Distribution -- helps to optimise all the tasks and activities carried out in sales, delivery and billing. Key elements are; pre-sales support, inquiry processing, quotation processing, sales order processing, delivery processing billing and sales information system.

Each of these Modules may have sub-modules designed for specific tasks as detailed below.

System-Wide Features -- SAP uses certain system wide features that should be understood at the outset. These are used to logically, safely and flexibly organize the data in business enterprise.

Customizing- is the configuring of the system to represent your organization's legal structure, reporting requirements and business processes. Internal reporting is a managerial tool in the daily operations. External reporting is required by governmental units controlling the legal structure of the corporation, such as, the IRS State taxing authorities, SEC etc.

Organizational Elements

Financial –
client is a legal and organizationally independent unit at the highest level in SAP.
company is an independent legal entity within a client
business areas are used to produce profit and loss statements and balanced sheets across marketing lines.

Materials Management
Purchasing units
Plants

Sales and Distribution
Sales organization
Distribution channel
Division

Master Data is records that remain in the database over an extended period of time. Examples:
Customer Master
Vendor Master
Material Master
Account Master

This structure eliminates redundant data and is shared by all SAP Modules. It is a critical aspect of the robustness of the system.

- Employee self service-your employees have access to their own HR records over the Internet
- Classification is the assignment of objects to a class. Each class has standard characteristic.
- Matchcodes are query tools used to find specific information using search methods.
- Security is administered for objects, profiles and authorizations. Users are only authorized to see or change the parts of the system required by their job responsibilities.

BUSINESS PROCESSES AND SAP FUNCTIONALITY

In order to understand a system like SAP a thorough understanding of the events and relationship that take place in a business is required. It is not enough to just realize the Sales, Production, Finance and Accounting have jobs to do in a business. The exact details of each action, the timing of that action and its interrelationships with every other process must be understood. In many large operations there may be no person that has a complete grasp of the situation.

Before an operation can be automated or computerized a thorough study of the business must be undertaken. This task is called Business Process Engineering.

Sequential Walk Through

Sales

Pre-sales activity-planning and availability support for the sales personnel

Sales Order- The actual entry of the sales order into the system done by the salesperson at the point of sales perhaps using a PC and Internet connections.

Determining where the most efficient source of the ordered product is in inventory and shipping it.

Delivery

Customer Billing

Customer Payment

Production

Sales and operations planning SOP where the sales forecasts are used in a production planning model to check feasibility.

Master Production Scheduling MPS-The actual plan for the whole production process

Material Requirements Planning MRP-Where the production plan is actually converted into raw materials input requirements.

Planned Order-When materials are available and capacity exists this plan is created and then converted into a production Order.

Shop Floor Control where the actual production takes place and is registered into the system as finished goods.

Purchasing

Requisition-Once the Production manager plans to manufacture something a requisition for the raw materials required but not on hand must be prepared.

Vendor Selection-made by the purchasing department.

Purchase order sent

Goods receipt increasing inventory

Invoice verification as it is received from vendor

Payment to vendor

Finance and accounting

Sales events must be captured at the proper time into the ledger system.

Inventory must be adjusted to match goods shipped.

Inventory must be adjusted to match raw materials received.

Inventory must be adjusted to move value from raw materials to work in process.

Inventory must be adjusted to increase finished goods when they are produced.

Accounts Payable must be set up for purchases.

Accounts Receivable must reflect goods billed but not yet paid for.

Business Process Engineering must not only identify all these steps but must also find the most efficient way to minimize redundant actions. For example, when sales are made inventory and manufacturing plans should be automatically updated. When manufacturing plans are updated raw materials should be automatically ordered from vendors. When finished goods are shipped customers

should be automatically billed at the same instance. Real situations are far more complex than the simple explanation above.

QUICK TOUR OF THE SAP USER INTERFACE

The SAP R/3 system presents a Windows interface with several of the familiar windows functions for screen manager. The apparent simplicity of the interface hides the power of the menus residing within the menubar at the top of the screen. The initial screen shows a menubar with the following selections. The first level sub menus are listed below to give you a idea of where to start.

Office
- Workplace
- Telephone Integration
- Appointment Calendar
- Room Reservations
- Start Workflow
- Business Documents

Logistics
- Materials Management
- Sales / Distribution
- Logistics Execution
- Production
- Production-Process
- Plant Maintenance
- Customer Service
- Quality Management
- Logis controlling
- Project Management
- Environment Health & Safety
- Central Functions

Accounting
- Financial Accounting
- Treasury
- Controlling
- Enterprise Control
- Investment Management
- Project Management
- Real Estate

Human Resources
- Managers Desktop
- Personnel admin.
- Time management
- Payroll
- Training and Event Management
- Organizational Management
- Travel
- Information system

Information Systems
- Executive Information Systems
- Logistics
- Accounting
- Human Resources
- Project System
- Ad Hoc Reports
- General Report System

Tools
- ABAP/4 Workbench
- Accelerated SAP
- Administration
- ALE
- Business Communication
- Business Framework
- Business Workflow
- CCMS
- Web Development
- SAP Script
- Hypertext
- Find.

Year of Exam	Question No.	Chapter No.	Ans. Page No.	Marks	Question
Nov-02	[4(a)]	12	12.2,12.5,12.17	10	What is an ERP system? Bring out the major challenges involved in its implementation
May-03	[4(b)]	12	12.14-12.15	10	Explain the process of evaluation of various ERP packages.
Nov-03	[5(b)]	12	12.16	8	Write down the general guidelines which are to be followed before starting the implementation of an ERP package.
Nov-03	[5(a)]	12	12.2	2	What is an ERP (Enterprise Resource Planning) system?
Nov-04	[5(a)]	12	12.17 - 12.18	10	Write a detailed note on the expectations, fears and the ground realities that a corporate management faces during the post-implementation phase of ERP.
Nov-04	[7(b)]	12	12.8	5	Write short note : Business Process Re-engineering
May-05	[6(a)]	12	12.5-12.6	5	What are the characteristics and features of an ERP?
May-05	[6(b)]	12	12.19-12.20	5	List any five ERP Vendors and briefly describe the ERP packages offered by them
Nov-05	[4(b)]	12	12.6-12.7	10	What are the benefits achieved by implementing the ERP packages?
Nov-05	[7(c)]	12	12.8	5	Business Engineering
May-06	[5(b)]	12	12.14-12.15	5	Explain the various criteria used for evaluation of the ERP packages.
Nov-06	[7(a)]	12	12.28-12.29	5	Enterprise Controlling

May-07	[2(b)]	12	12.18-12.19	10	How will you establish and implement Critical Success Factors (CSFs) and key Performance Indicators (KPIs) un an organisation for achieving the benefits of implementations of ERP?
Nov-07	[6(a)]	12	12.5-12.7	10	What is Enterprise Resources Planning? Briefly describe its benefits.
May-08	[4(a)]	12	12.5-12.6	5	Briefly explain the characteristics and features of an Enterprise Resource Planning.
Nov-08	[3(b)]	12	12.25-12.26	5	Discuss the functions and facilities provided by Treasury Cash Management module of an ERP package.

Chapter XIII: *CONTROLS IN EDP SET-UP : GENERAL CONTROLS*

1. General Controls :

These controls apply to a wide range of exposures that systematically threaten the integrity of all applications processed within the Computer Based Information System (CBIS) environment. General controls can be further subdivided under following headings:

Operating System: Is the computer control program. It allows users and their applications to share and access computer resources such as processors, databases, printers, etc.

(i) Functions of operating system
1. Translation of High level language that the computer can execute.
2. Allocation of computer resources
3. Job scheduling and multiprogramming.

(ii) Control objectives of operating system
1. The operating system must protect itself from users
2. Must protect users from each other
3. Must protect users from themselves
4. Must be protected from itself
5. Must be protected from its environment

(iii) Operating System Security

Log-On Procedure: When the user initiates the process, he or she is presented with a dialog box requesting the user's ID and password. The system compares the ID and password to a database of valid users. If the system finds a match, then the log-on attempt is authenticated. If, however, the password or ID is entered incorrectly, the log-on attempt fails and a message is returned to the user. The message should not reveal whether the password or the ID caused the failure. The system should allow the user to reenter the log-on information. After a specified number of attempts (usually not more than five), the system should lock out the user from the system.

Access Token: Creates an access token that contains key information about the users, including user ID, password, user group, and privileges granted to the user. The information in the access token is used to approve all actions attempted by the user during the session.

Access Control List: Access to system resources such as directories, files, programs, and printers are controlled by an access control list assigned to each resource. These lists contain information that defines the access privileges for all valid users of the resource. When a user attempts to access a resource, the system compares his or her ID and **priviliges contained in the access token with those contained in the access control list.** If there is a match, the user is granted access.

Discretionary Access Control: In distributed systems, however, resources may be controlled (owned) by end users. Resource owners in this setting may be granted discretionary access control, which allows them to grant access privileges to other users. E.g. the controller who is the owner of general ledger grants only read only privilege to the manager in budgeting department.

(iv) Threats to Operating System Integrity:

Accidental threats:

It include hardware failures that cause the operating system to crash. Accidental system failures may cause whole segments of memory to be "dumped" to disks and printers, resulting in the unintentional disclosure of confidential information

Intentional threats:

1) Privileged personnel who abuse their authority e.g. system administrator and programmers.
2) Individuals, both internal and external to the organisation, who browse the operating system to identify and exploit security flaws.
3) An individual who intentionally (or accidentally) inserts a computer virus or other form of destructive program into the operating system.

(v) Controlling Access Privileges:

Reusable Passwords: The user defines the password to the system once and then reuses it to gain future access. Most operating systems set only basic standards for password acceptability. To improve access control, management should discourage the use of "weak" passwords. Inexpensive software is available that automatically scans password files and notifies security administrator when a weak password is detected ensuring that only smart passwords are used.

One-time Passwords: To access the operating system, the user must provide both a secret reusable personal identification number (PIN) and the current one-time-only password for that point in time.

(vi) Viruses and other Threats

Virus: A virus is a program (usually destructive) that attaches itself to a legitimate program to penetrate the operating system. One common technique is for the virus to simply replicate itself over and over within the main memory, thus destroying whatever data or programs are resident. When a virus-infected program is executed, the virus searches the system for uninfected programs and copies itself into these programs. The virus in this way thus spreads to the applications of other users or to the operating system itself.

Worm: Viruses attach themselves to other legitimate programs, however, worms usually exist as separate, independent programs. Worms use operating system services as their means of replication.

Logic Bomb: A logic bomb is a destructive program, such as a virus, that is triggered by some predetermined event. E.g. the famous Michelangelo virus (triggered by his birthdate) is an example of logic bomb.

Back Door: A back door (also called a trap door) is a software program that allows unauthorized access to a system without going through the normal (front door) log-on procedure. The purpose of the back door may be to provide easy access to perform program maintenance, or it may be to perpetrate a fraud or insert a virus into the system.

Trojan Horse: Purposefully hidden malacious or damaging code within an authorised computer program. e.g. The program is designed to mimic the normal log-on procedures of the operating system. When the user enters his or her ID and password, the Trojan horse stores a copy of them in a secret file. At some late date, the author of the Trojan horse uses these Ids and passwords to access the system and masquerade as an authorized user.

Controlling Against Viruses and other Destructive Programs:

- Purchase software only from reputable vendors and accept only those products that are in their original, factory-sealed packages.
- Examine all upgrades to vendor software for viruses before they are implemented.
- Establish an educational program to raise user awareness regarding viruses and malicious programs.
- Install all new applications on a stand-alone computer and thoroughly test them with antiviral software prior to implementing them on the mainframe or LAN server.
- Routinely make back copies of key files stored on mainframes, serves, and workstations.
- Use antiviral software (also called vaccines) to examine application and operating system programs for the presence of a virus and remove it from the affected program. The software

works only on known viruses. It is therefore important to maintain the current version of the vaccine.

(vii) Controlling Audit Trails

What is Audit Trails?
Audit trails are logs that can be designed to record activity at the system, application, and user level. Many operating systems allow management to select the level of auditing to be provided by the system. This determines which events will be recorded in the log.

Objectives of Audit Trials
1. Detecting Unauthorized Access: It can occur in real time or after the fact. The primary objective of real-time detection is to protect the system from outsiders who are attempting to breach system controls. A real-time audit trail can also be used to report on changes in system performance that may indicate infestation by a virus or worm. After the fact Audit logs can be used to determine if unauthorized access was accomplished, or attempted and failed.
2. Reconstructing Events: It can be used to reconstruct the steps that led to events such as system failures. Knowledge of the conditions that existed at the time of a system failure can be used to assign responsibility and to avoid similar situations in the future.
3. Personal Accountability: To monitor user activity at the lowest level of detail. This capability is a preventive control that can be used to influence behavior. Individuals are least likely to violate organisations security policy if they know that their actions are recorded on audit log.

Data Management Controls

(i) Access Controls:
Access Controls are designed to prevent unauthorized individuals from viewing, retrieving, corrupting, or destroying the entity's data.
a. User View: It is a subset of the total database that defines the user's data domain and provides access to the database. Access privileges to the data, as defined in their views, should be commensurate with the user's legitimate needs. Although a user view can restrict the user access to a limited set of data, they do not define task privileges, such as read, delete or write.
Comment:- Different authority levels not taken care of.
b. Database Authorization Table: This technique is similar to the access control list used in the operating system. Each user is granted certain privileges that are coded in the authority table, which is used to verify the user's action requests.
c. User-defined Procedures: A user defined procedure allows the user to create a personal security program or routine to provide more positive user identification than a single password can.
d. Data Encryption: Data encryption uses an algorithm to scramble selected data, thus making it unreadable to an intruder "browsing" the database. In addition to protecting stored data, encryption is used for protecting data that are transmitted across networks.
e. Biometric Devices: The ultimate in user authentication procedures is the use of biometric devices, which measure various personal characteristics, such as fingerprints, voice prints, retina prints, or signature characteristics. These user characteristics are digitized and stored permanently in a database security file or on an identification card that the user carries. When an individual attempts to access the database, a special scanning device captures his or her biometric characteristics, which is compared with the profile data stored internally or on the ID card.

Back-up Controls

To recover from disasters, organisations must implement policies, procedures and techniques that systemically and routinely provide backup copies of critical files. Often, the originals are stored at site that is physically distant from the actual site, and where duplicate copies are used for processing. The backup copies must be kept in a place which is not susceptible to the same hazards as the originals.

(i) Technique of File reconstruction

Magnetic Disk: Contents of master file on magnetic disk are periodically copied or dumped on magnetic tape backup file and stored at another location. A record of transactions is also maintained separately on magnetic tapes to serve two purposes. First, as the transactions occur constantly, this record provides a link from one backup file to another. Second, as writing on magnetic disks occurs by overlying technique, the record of transactions helps in providing particulars of all records that caused a change to the magnetic disk file. In the case of system going down or the master file getting destroyed, the reconstruction can be carried out.

Magnetic Tapes (Son-Father-Grandfather technique): Master Files relating to Two previous periods are retained in addition to current updated master file and current transaction file. This is also called as Son-Father-Grandfather technique.

(ii) Backup Controls in the Database Environment
This system provides four backup and recovery features: database backup, a transaction log, checkpoints, and a recovery module. Each of these is described below.

Backup: The backup feature makes a periodic backup of the entire database.

Transaction log (Journal): It provides an audit trail of all processed transactions. It lists transactions in **a transaction log file** and records the resulting changes to the database in a separate **database change log**.

Checkpoint Feature: The checkpoint facility suspends all data processing while the system **reconciles the transaction log and the database change log against the database**. At this point, the system is in a "quiet state". Checkpoints occur automatically several times an hour. If a failure occurs, it is usually possible to restart the processing from the last checkpoint. Thus, only a few minutes of transaction processing must be repeated.

Recovery Module: The recovery module uses the logs and backup files to restart the system after a failure.

Organisation Structure Controls:

(i) Separating Systems Development from Computer Operations:
With detailed knowledge of the application's logic and control parameters and access to computer functions, an individual could make unauthorized changes to the application during its execution. Such changes may be temporary and may disappear without a trace when the application terminates.

(ii) Separating the Database Administrator from Other Functions:
The DBA is responsible for a number of critical tasks pertaining to database security, including creating the database schema, creating user subschemas (views), assigning access authority to users, monitoring database usage, and planning for future expansion. Delegating these responsibilities to other persons who perform incompatible tasks threatens database integrity.

(iii) Separating New Systems Development from Maintenance:
Some companies organize their systems development function into two groups: systems analysis and programming. Although a popular arrangement, this approach promotes two types of control problems: inadequate documentation and fraud.

(iv) Separating the Data Library from Operations:
The data library provides safe storage for the off-line data files, such as magnetic tapes and removable disk packs. The librarian must keep a detailed log of each file, including file name, serial number, contents, creation date, and retention dates. The librarian issues scratch tapes (when their expiration dates are exceeded) to computer operators in accordance with system requests. When the program run is complete, the operator returns the file (s) to the librarian for storage. Management should maintain strict control over who performs library functions to ensure that these responsibilities are not assumed by other operators during busy periods.

System development Controls:

1. System Authorization Activities: All systems must be properly authorized to ensure their economic justification and feasibility. This requires that each new system request be submitted in written form by users to systems professionals who have both the expertise and authority to evaluate and approve (or reject) the request.

2. User Specification Activities: Users must be actively involved in the systems development process. Regardless of the technology involved, the user can create a detailed written description of the logical needs that must be satisfied by the system. This document remain a statement of user needs.

3. Technical Design Activities: The technical design activities in the SDLC translate the user specifications into a set of detailed technical specifications of a system that meets the user's needs. The adequacy of these activities is measured by the **quality of the documentation** that emerges from each phase. Documentation is both a control and evidence of control and is critical to the system's long term success.

4. Internal Audit Participation: The internal auditor plays an important role in the control of systems development activities particularly in organisations whose users lack technical expertise. The auditor should become involved at the inception of the SDLC process to make conceptual suggestions regarding system requirements and controls.

5. Program Testing: All program modules must be thoroughly tested before they are implemented. Test data prepared during the implementation phase must be preserved for future use.

6. User Test and Acceptance Procedures: A test team comprising user personnel, systems professionals, and internal audit personnel subjects the system to rigorous testing. The formal test and acceptance of the system are considered by many to be the most important control over the SDLC. It is imperative that user acceptance be documented. Before implementation, this is the last point at which the user can determine the system's adequacy and acceptability.

Systems Maintenance Controls:

1. Maintenance Authorisation, Testing, and Documentation: All maintenance actions should require minimum four controls: formal authorizations, technical specifications, testing, and documentation updates.

2. Source Program Library Controls: In larger computer systems, application program modules are stored in source code form on magnetic disks called the source program library (SPL)

The Worst Case Situation – No Controls

1. Access to program is completely unrestricted. Programmers and others can access any programs stored in the library, and there is no provision for detecting an unauthorised intrusion.
2. Because of these control weaknesses, programs are subject to unauthorized changes. Hence, there is no basis for relying on the effectiveness of other controls

A Controlled SPL Environment:

This requires the implementation of an SPL management system (SPLMS).
This software is used to control four routine but critical functions:

1. Storing programs on the SPL,
2. Retrieving programs for maintenance purposes,
3. Deleting obsolete programs from the library, and
4. Documenting program changes to provide an audit trail of the changes.

Mere presence of an SPLMS does not guarantee program integrity. An SPL requires specific planning and control techniques to ensure program integrity.

Password Control:
One form of access control over the SPL is provided by assigning passwords. When more than one person is authorized to access a program, preserving the secrecy of a shared password is a problem.

Separation of Test Libraries: An improvement on the shared password approach through the creation of separate password-controlled library for each programmer. Production programs are copied into the programmer's library for maintenance and testing purposes only. Direct access to the production SPL is limited to a specific librarian group that must approve all requests to modify, delete, and copy programs. Passwords for production programs can be changed regularly and disclosed only on a need-to-know basis.

3. Audit Trail and Management Report:
Program modification reports, which describe in detail all program changes (additions and deletions) to each module. These reports should be part of the documentation file of each application to form an audit trail of program changes over the life of the application

4. Program Version Number:
The SPLMS assigns a version number automatically to each program stored on the SPL. When programs are first placed in the libraries (at implementation), they are assigned a version number of zero. With each modification to the program, the version number is increased by one. For instance, after five authorized maintenance changes, the production program will be Version 05. This feature, when combined with audit trail reports, provides evidence for identifying unauthorized changes to program modules. An unauthorized change is signaled by a version number on the production load module that can not be reconciled to the number of authorised changes.

5. Controlling Access to Maintenance Commands:
Powerful maintenance commands are available for most library systems that can be used to alter or eliminate program passwords, alter the program version (modification) number, and temporarily modify a program without generating a record of the modification. If not controlled, maintenance commands open the possibility of unrecorded, and perhaps unauthorized program modifications.

6. Message sequence numbering:
An intruder in communication channel may attempt to delete a message from stream of messages, change order of messages received, duplicate a message, etc. Through message sequence numbering, a sequence number is inserted in each message and any attempt will become apperant at receiving end.

Computer Centre Security and Control:

a. Fire damage:
1. Automatic and manual fire alarms.
2. Sprinkler systems are recommended when a computer room contains an appreciable amount of combustible material. Halogen gas which requires no clean up. Smoke detectors can be placed below the raised floor.
3. An appropriate type of manual fire extinguishers.
4. The building may be constructed from fire resistant materials.
5. Fire extinguishers and fire exits should be marked clearly.
6. When a fire alarm is activated, a signal may be sent automatically to a permanently manned station.

b. Water damage:
It can be the outcome of a fire.
1. Waterproof ceilings, walls and floors.
2. Ensure an adequate drainage system exists.
3. Install alarms
4. Installation above the high water level.
5. Master switch for all water mains.
6. Dry pipe automatic sprinkler system that is charged by an alarm and activated by the fire.
7. Cover hardware with a protective fabric when it is not in use.

c. Energy variations:
Voltage regulators protect hardware against temporary circuit breakers protect the hardware against sustained increase. Battery back up can be provided in case a temporary loss of power occurs.

d. Pollution damage:
The major pollutant is dust, filtering of air passing

e. Unauthorized intrusion:
The intruder physically may enter the installation to steal assets or carry out sabotage. Eavesdrop on the installation by wire-tapping, installing an electronic bug or using a receiver that picks up electro-magnetic signals. Eavesdropping breaches the privacy of data. Various devices are available to detect the presence of bugs.

f. Disaster Recovery Plan
1. Emergency Plan: Outlines the actions to be undertaken immediately after a disaster occurs. The personnel to be notified immediately. It provides guidelines on shutting down equipment.
2. Recovery Plan: DRP sets outs how the full capabilities will be restored. A recovery committee is constituted. Setting out priorities for recovery of application systems, hardware replacement etc. will be the responsibility of Recovery Committee.
   (i) An inventory of the hardware, application systems, system software, documentation etc. must be taken.

(ii) Criticality of application system and the importance of and indication must be given of the efforts and cost involved in restoring the various application systems.
(iii) An application systems hierarchy must be spell out
(iv) Selection of a disaster recovery site must be made.
(v) A formal backup agreement with another company must be made.

3. Backup Plan:
Organisations no matter how physically secure, their systems are always vulnerable to the disaster. Therefore, an effective safeguard is to have a backup of anything that could be destroyed, be it hardware or software. The backup copies must be kept in a place which is not susceptible to the same hazards as the originals.

4. Test plan:
This plan looks after the testing of DRP and analysis of the result. It identifies deficiencies in the emergency, backup or recovery plan

a. Plan walk-throughs: Critical personnel in the plan's execution reasoning out what might happen in the event of the different disasters
b. Localised tests: It simulates system crash.
c. It is nearer to disaster conditions. Paper walkthrough and localised tests should have been conducted before completely shutting down the operations to simulate disasters.

g. Insurance:
Risk to computer system can be controlled through system design installation of security measures and regular security audit. Residual risk is to transfer it contractually to a third party by way of insurance of the computer installation. Management must be careful to ensure that they consider all major potential losses; the replacement cost of purchased or leased hardware must be covered, special construction relating to raised floors and air conditioning must be covered etc.

Internet and Intranet Controls:

There are two major exposures in the communication subsystem. First data may be lost or corrupted through component failure. Second, a hostile party, intruder may seek to subvert data being transmitted through the subsystem.

1. Component failure:
a) Communication lines b) Hardware c) Software

2. Subversive threats:
a. Invasive tap: By installing it on communication line, he can read & modify data.
b. Inductive tap: It monitors electromagnetic transmissions and allows the data to be read only.

Ways of Manipulating message:
a. Insert a message
b. Delete a message
c. Modify the contents
d. Duplicate messages
e. Deny message services between a sender and a receiver
f. Spurious associations. They may play back a handshaking sequence.

Controlling risk from Subversive Threats
a. Fire walls: A firewall is a system that enforces access control between two networks.
All traffic between the outside network and the organisation's Intranet must pass through the firewall.
Only authorised traffic between the organisation and the outside, as specified by formal security policy, is allowed to pass through the firewall.
The firewall must be immune to penetration from both outside and inside the organisation.

Network-level firewalls provide low cost and low security access control. This type of fire wall consists of screening router that examines the source and destination addresses that are attached to incoming message packets. The firewall accepts or denies access requests based on filtering rules that have been programmed into it.

Application-level firewalls provide a high level of customizable network security, but can be extremely expensive. These systems are configured to run security applications called proxies that permit routine services such as e-mail to pass through the firewall, but can perform sophisticated functions such as logging or user authentication for specific tasks.

b. Controlling Denial of service Attacks
Computer hackers and crackers have devised a malicious act called a denial of service attack, in which the attacker transmits hundreds of SYN packets to the targeted receiver but never responds with an ACK to complete the connection. The ports of the receiver's server are clogged with incomplete communication requests that prevents legitimate transactions from being received and processed. Such attacks are difficult to prevent because IP spoofing is used to disguise the source of the message. Internet sites with firewalls must engage in a policy of social responsibility. The firewalls at source site can be programmed to block messages with non-internal addresses. Security software is available for the targeted sites that scan for half open connections. The software looks for SYN packets that have not been followed by an ACK packet. The clogged ports can then be restored to allow legitimate connections to be made.

c. Encryption
i) Private Key Encryption – Data Encryption Standard (DES) algorithm uses a single key to do both, i.e. Encrypt and Decrypt the message
ii) Public Key Encryption – This technique uses two different keys: one for encoding messages and other for decoding them.

d. Message transaction Log
All incoming and outgoing messages, as well as attempted (failed) access, should be recorded in a message transaction log

e. Call back Devices
A call back device requires the dial in user to enter a password and be identified. The system then breaks the connection to perform user authentication. If the caller is authorized, the call back device dials the caller's number to establish a new connection. This limits access from only authorized terminals or telephone numbers and prevents an intruder masquerading as a legitimate user.

Personal Computer Controls:

Special characteristics of PCs that give rise to new risks:

- They are small, fast and powerful. Some of them even approach the power of minis and mainframes.
- They are available in many makes and model.
- Floppies provide a convenient way of data storage.
- Their user-friendliness has resulted in end – user computing.
- They acts as an expensive front – ends to large computers.
- They is a tendency to buy off –the shelf application package.
- They are prone to virus infection.

The resultant new security risks are as follows:

- PC's are likely to be shifted from one location to another or even taken outside the Organisation.
- Decentralized purchasing of PC's can result in hardware incompatibility in the long run.
- Floppies can be very conveniently transported from one place to another, as a result of which data corruption may occur. Mishandling, improper storage etc. can also cause damage.
- The inherent data security provided is rather poor.
- There is a chance that applications software are not thoroughly tested.
- Segregation of duties is not possible, owing to limited number of staff.
- The operating staff may not be adequately trained.
- Computer viruses can slow down the system, corrupt data and so on.

The security measures that could be exercised are as follows:

- Physically locking the keyboard or the PC itself must be enforced.
- Proper logging of equipment shifting must be done.
- The PC purchases must be centrally coordinated and company-wide standards established for spread sheets, word-processors, applications software etc.
- Floppies must be stored in secured places and their issues duly authorized. They must be adequately packed before shipment.
- Data and programs on hard-disks must be secured before using hardware/software mechanisms. Backup must be taken regularly.
- Minimum standards must be set for developing, testing and documenting applications.
- Properly organised training programs must be periodically conducted. More than one user should be trained on each application.
- Virus prevention and detection software obtained from reliable sources must be used. Write protect tabs must be used on diskettes that do not require any alteration. Private software should be strictly avoided.
- The PC's and their peripherals must be maintained regularly.
- While the proliferation of powerful PC's in recent years has its own plus points, the associated risks must be ignored. Thus, implementing effective controls is of prime importance.

Weak Access Control:

Disk locks are devices that prevent unauthorized individuals from accessing the floppy disk drive of a computer. One form of disk lock is a memory – resident program that prevents the computer from being booted from A: drive. The lock will also prevent the A: drive from being used to run programs, upload data and programs to the hard disk or download from the hard disk. This form of disk lock is password controlled so it can be disabled as needed by an authorized user.

With a memory-resident disk lock in place, the user may be denied access to the A: drive. Being unable to boot from either device permanently access to data and programs. An alternatively solution is to use a physical disk lock rather then the memory-resident type. This device fits into A: drive like a floppy disk to prevent its use and is secured with a physical lock and key.

Multilevel Password Control:

This technique uses stored authorization tables to further limit an individual's access to read-only, data input, data modification and data deletion capability.

Inadequate Backup Procedures:

In mainframe and network environment, back up is controlled automatically by operating system, using specialized software and hardware. The responsibility of providing back up in the PC environment falls to the user. Computer failure, usually disk failure, is primary cause of significant data loss in the PC environment.

Floppy Disk Back Up:
Files can be backed up to floppy disks at routine periods during processing and stored away from the computer.

Dual Internal Hard Drive:
Microcomputers can be configured with two physical internal hard disks. One disk can be used to store production data while the other stores the backup files. A batch program, run prior to or immediately after each data processing session, can be copy the data file to the backup disk. Thus, backup is almost transparent to the user and involves a minimum effort.

External Hard Device:
A popular backup option is external hard device with removable disk cartridge, which can store more than a gigabyte of data per cartridge.

Tape Backup Device:
The most common type of archive device for PCs is magnetic tape. These may be internal or external device and provide efficient and inexpensive backup. In normal backup mode, a single tape can stored about 1.6gigabytes of data. In compressed mode, a tape can store up to 3.2 gigabytes.

Year of Exam	Question No.	Chapter No.	Ans. Page No.	Marks	Question
Nov-02	[1(b)]	13	13.29-13.34	10	What are the two major categories of exposures in the Communication subsystems including Internet and Intranet? What control mechanisms could be used to deal with them?
May-03	[7(e)]	13	13.34,13.35-13.36	5	Wtite short note : Personal Computer Controls
Nov-03	[1(d)]	13	13.23-13.26	10	What are the different types of securities required for the computer system? Explain briefly the different components of physical security of a computer installation.
May-04	[4(a)]	13	13.18-13.19	10	Discuss the activities dealing with system development controls in EDP setup.
May-04	[7(c)]	13	13.30-13.31	5	Write short note : Firewalls
Nov-04	[7(c)]	13	13.32 - 13.33	5	Write short note : Encryption
May-05	[5(a)]	13	13.26-13.28	10	What do you understand by disaster recovery plan? Discuss its various components.
May-05	[4(c)]	13	13.913.11	5	Describe various access control methods used for safety of the database.
Nov-05	[1(c)]	13		5	"No Company, big or small, can ignore the opportunity opened by the internet" What are the various methods by which internet can be accessed? What are the considerations for choosing the right alternatives?
Nov-05	[1(d)]	13		5	Mention any five security steps an internet user should take to protect from cyber crime and computer security threats
Nov-05	[5(b)]	13	13.8	5	Discuss various ways in which audit trail can be used to support security objectives?
May-06	[6(b)]	13	13.3-13.4	5	Describe the various security components available in secure Operating system.

May-06	[7](i)	13	13.30-13.31	5	Write Shot notes on any four of the following: (i) Firewalls
May-06	[7](iv)	13	13.20-13.22	5	Write Shot notes on any four of the following: (iv) Source program library control
Nov-06	[1(c)]	13	13.1-13.2	5	Differentiate between General and Application controls. Also mention the broad categories into which the first can be subdivided.
Nov-06	[5(c)]	13	13.29-13.30	5	What are the subversive threats? How do the intruders manipulate the message being transmitted?
May-07	[4(b)]	13	13.2-13.3	5	What are five control objectives of an Operating system?
Nov-07	[5(b)]	13	13.13-13.14	5	State and explain the four back up and recovery features necessary in a DBMS
May-08	[1(c)]	13	13-9-13.11	5	Briefly discuss any five database control features.
May-08	[6(c)]	13	13.20-13.23	5	Discuss how a controlled source program library environment can help to deter unauthorized changes to program.
May-08	[7(d)]	13	13.30-13.31	5	Write short note: Firewalls.
Nov-08	[6(a)]	13	13.26-13.28	10	What is 'Disaster Recovery Plan'? Discuss its various components.
Nov-08	[7(a)]	13	13.32-13.33	5	Write short note : Encryption techniques

Chapter XIV: *CONTROLS IN EDP SET-UP: APPLICATION CONTROLS*

1. Application controls

Application controls deal with exposures within specific applications, such as payroll, purchases, and cash disbursements systems. Fall into three broad categories: input controls, processing controls, and output controls.

2. Input Controls

Input Controls at this stage attempt to ensure that these transactions are valid, accurate, and complete.

a. Source Document Controls: In systems that use physical source documents to initiate transactions, careful control must be exercised over these instruments.
   (i) Use Pre numbered Source Documents:
   (ii) Use Source Documents in Sequence
   (iii) Periodically Audit Source Documents

b. Data Coding Controls: Coding controls are checks on the integrity of data codes used in processing.

Errors:
(i) Addition errors occur when an extra digit or character is added to the code.
(ii) Truncation errors occur when a digit or character is removed from the end of a code.
(iii) Substitution errors are the replacement of one digit in a code.
(iv) Transposition errors are of two types
Single transposition errors occur when two adjacent digits are reversed.
Multiple transposition errors occur when nonadjacent digits are transposed.

Controls:
(i) Check Digits: A check digit is a control digit (or digits) added to the code when it is originally assigned that allows the integrity of the code to be established during subsequent processing. The check digit can be located anywhere in the code, as a prefix, a suffix, or embedded someplace in the middle. Whenever the code is transcribed from one document to another this check is to be effected.
(ii) Batch Controls: The objective of batch control is to reconcile output produced by the system with the input originally entered into the system. This provides that:
All records in the batch are processed.
No records are processed more than once.
An audit trail of transactions is created from input through processing to the output stage of the system.
Two documents are used to accomplish this task: a batch transmittal sheet and a batch control log. The batch transmittal sheet captures relevant information about the batch, such as: A unique batch number, A batch date, A transaction code (indicating the type of transactions, such as a sales order or cash receipt),The number of records in the batch (record count), The total amount value of a financial field (batch control total), The total of a unique non-financial field (hash total)
The batch transmittal sheet is prepared by the user department and is submitted to data control along with the batch of source documents. The data control clerk receives transactions from users assigns each batch a unique number, date-stamps the documents, recalculates the batch control numbers, such as the total amount of the batch and a hash total (discussed later). The clerk enters the batch control information in the batch control log and submits the batch of documents along with the transmittal sheet, to the data entry department. The data entry group codes and enters the transmittal sheet data onto the transaction file, along with the batch of transaction records. The transmittal sheet becomes the batch control record and is used to asses the integrity of the batch during processing.

(iii) Validation Controls: Input validation controls are intended to detect errors in transaction data before the data are processed.

a. Field Interrogation: Procedures that examine the characters of the data in the field.

(i) Limit checks: The field is checked by the program to ensure that its value lies within certain predefined limits.

(ii) Picture checks: These check against entry into processing of incorrect characters.
Example: All department numbers may be made up of numeric. An incorrect deptt. No.4D3 would thus be filtered.

(iii) Valid Code checks: Checks are made against predetermined transactions codes tables or order data to ensure that input data are valid.

(iv) Check Digit:

(v) Arithmetic checks: Arithmetic is performed in different ways to validate the result of other computations of the values of selected data fields.
Example: In payroll processing it is usual to accumulate gross pay, deduction and net pay. At each employee's record whenever those totals are accumulated, the gross pay must equal net pay + deductions.

(vi) Cross Checks: may be employed to verify fields appearing in different files to see that the result tally. For example the quantity received quantity invoiced by the supplier and quantity ordered may be compared.

b. Record interrogation

1. Sequence checks are exercised to detect any missing transaction, off serially numbered vouchers
2. Format completeness checks are used to check the presence and position of all the fields in a transaction.
3. Combination checks are used to check such combinations that could be invalid.
4. Passwords are issued to the various users in on-line systems for processing their inquiries.

c. File Interrogation:
The purpose of file interrogation is to ensure that the correct file is being processed by the system.
Internal label checks verify that the file processed is the one the program is actually calling for. The system matches the file name and serial number in the header label with the program's file requirements. If the wrong file has been loaded, the system will send a message to the operator and suspend processing.
Version checks are used to verify that the version of the file being processed is correct.
An **expiration date check** prevents a file from being deleted before it expires.

3. Input error correction:

When errors are detected in a batch, they must be corrected and the records should be resubmitted for reprocessing.
Immediate correction: If the system is using the direct data validation approach, error detection and correction can also take place during data entry.
Create an Error File: Individual errors are flagged to prevent them from being processed. At the end of the validation procedure, the records flagged as errors are removed from the batch and placed in a temporary error holding file until the errors can be investigated.
Errors detected during processing require careful handling. These records may already be partially processed. There are two methods for dealing with this complexity. The first is to reverse the effects of the partially processed transactions and resubmit the corrected records to the data input stage. The second method is to reinsert corrected records to the processing stage in which the error was detected.

Reject the Batch: Some forms of errors are associated with the entire batch and are not clearly attributable to individual records. An example of this type of error is an imbalance in a batch control total. The most effective solution in this case is to cease processing and return the entire batch to data control to evaluate, correct, and resubmit.

4. Processing Controls

4.1 Run to Run Controls:

Run to run control use batch figures to monitor the batch as it moves from one programmed procedure (run) to another. These controls ensure that each run in the system processes the batch correctly and completely.

Recalculate Control Totals:
After each major operation in the process and after each run, amount fields, hash totals and record count are accumulated and compared to the corresponding value stored in the control record. If a record in the batch is lost, goes unprocessed, or is processed more than once, this will be revealed by the discrepancies between these figures.

Transaction Codes:
The transaction code of each record in the batch is compared to the transaction code contained in the control record. This ensures that only the correct type of transaction is being processed.

Sequence Checks:
In systems that use sequential master files, order of the transaction records in the batch is critical to correct and complete processing. As the batch moves through the process, it must be restored in the order of the master file used in each run. The sequence check control compares the sequence of each record in the batch with the previous record to ensure that proper sorting took place.

4.2 Operator Intervention Control:

System sometimes require operator intervention to initiate certain actions, such as entering total control for the batch of records, providing parameter value for logical operation, and activating the program from a different point when reentering semi-processed error records. Operator intervention increases the potential of human error. Systems that limit operator intervention through operator's intervention control are thus less prone to processing error. Although it may be impossible to eliminate operator involvement completely, parameter values and program start points should, to the extent possible, be derived logically or provided to the system through look-up table.

4.3 Audit Trail Controls:

Transaction Logs: every transaction successfully processed by the system should be recorded on a transaction log, which serves as journal. There are two reasons for creating a transaction log. First, the transaction log is a permanent record of transactions. The validated transaction file produced at the data input phase is usually a temporary file. Once processed, the records on this file are erased (scratched) to make room for the next batch of transactions.
Second, not all of the records in the validated transaction file may be successfully processed. Some of these records may fail tests in the subsequent processing stages. A transaction log should contain only successful transactions- those that have changed account balances. Unsuccessful transactions should be placed in on error file. The transaction log and error files combined should account for all the transactions in the batch. The validated transaction file may then be scratched with no loss of data.
Transaction Listings: The system should produce a (hard-copy) transaction listing of all successful transactions. These listings should go to the appropriate users to facilitate reconciliation with input.

Log of Automatic transaction: Some transactions are triggered internally by the system. An example of this is when inventory drops below a preset recorder point, and the system automatically processes a purchase order. To maintain an audit trail of these activities, all internally generated transaction must be placed in a transaction log.

Listing of Automatic Transaction: To maintain control over automatic transactions processed by the system, the responsible end user should receive a detailed listing of all internally generated transactions.

Unique Transaction Identifier: Each transaction processed by the system must be uniquely identified with a transaction number. This is the only practical means of tracing a particular transaction through a database of thousand or even million of records. In system that use physical source documents, the unique number printed on the document can be transcribed during data input and used for this purpose. In real-time systems, which do not use source documents, each transaction should be assigned a unique number by the system.

Error Listing: A listing of all error records should go to appropriate user to support error correction and resubmission.

5. Output Controls

The two output controls we shall discuss here: (1) Tape and disk output controls, and (2) printed output controls.

1. **Tape and Disk Output Controls: -** Computer output to magnetic tapes and disks is not normally verified by direct human observation, as is the case with manually printed output. Hardware controls such as parity bit checking and software controls such as check digits can be carried out along with the information output transmission to make sure that no digits are lost in the communication process. It may be noted that the disk drives and tape drives have built-in dual recording mode to enable these machines to check on recording accuracy. It works as follows **:-**

   The disk/tape is encoded with the desired information, this information is read again using the reading mechanism of the tape or disk drive. A comparison is made to verify the original output. In most cases, the comparison of the initial output data with the newly recorded data will result in a confirmation of identical information, and the tape or disk system is then able to signal the CPU that the required writing operation has been successful. This is called the ECHO check.

2. **Output Controls for Printed Output :** The main requirements and techniques of output controls for printed output may be considered under the headings :-
   (a) Verification of output;
   (b) Distribution of output;
   (c) Procedures for acting on exception reports.

(a) Verification of Output :-

1. **Output directly related to input: -** It includes some fields like serial number, name, address which do not change from input to output, because no calculation is performed in these fields.

2. **Output indirectly related to input: -** It includes those output fields which are outcome of calculation like addition, subtraction on some of fields like Gross pay = Basic pay + Allowance and Net pay = Gross pay – Deductions.

3. **Exception reports: -** These would include reports of items identified by the computer programs from a scrutiny on input data or master files not satisfying conditions specific in the program. For example Net Pay in excess of a specified amount, or slow-moving stock. Their complete and accurate production almost always depends on the correct functioning of the computer program.

(b) **Distribution of Output: -** If the user department that verifies the controls also acts on the output it will be apparent to the user department whether it received all that output. If however, the verification is carried out in the computer department or the output is not verified with the controls established over input or master file (e.g., exception reports), procedures often take the form of output registers or the sequential numbering of exception reports, to ensure that user department has received all outputs intact.

(c) **Procedures for Acting on Exception Reports: -** Exception reports often provide the information on which important control functions are based (e.g., control of overtime). A high degree of controls is thus usually required over the investigation of exception reports and the resulting action taken. This will often take the form of an independent review of exception reports to ensure that the exceptional items are promptly investigated and acted upon.

Year of Exam	Question No.	Chapter No.	Ans. Page No.	Marks	Question
Nov-03	[7(e)]	14	14.16-14.17	4	Write Short Note : Transaction logs
May-04	[4(b)]	14	14.2-14.3	5	What type of errors can corrupt a data code?
May-05	[7(a)]	14	14.16-14.17	5	Write short notes on: Transaction logs
Nov-05	[5(c)]	14	14.2	5	Explain the importance of sources documents and associated control techniques.
May-06	[5(a)]	14	14.6-14.12	10	What is the significance of input validation control? Describe briefly three different levels of input validation controls used in computerized information system
Nov-06	[1(b)]	14	14.7-14.9	5	Discuss some common types of field interrogation as a validation control procedures in an EDP set up.
May-07	[1(a)]	14	14.16-14.17	5	Briefly describe the techniques used to preserve audit trails in a Computer Based Information system
Nov-08	[7(c)]	14	14.16-14.17	5	Write short note : Audit trail controls in Computer Based Information System (CBIS)

Chapter XV: *DETECTION OF COMPUTER FRAUDS*

1. What is computer fraud?

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

Computer fraud would include:

a) Investment Frauds on the Internet involve the offering of unrealistically high returns on investment. Secret market frauds are variation on this theme. Victims are persuaded that there is a confidential and exclusive market for a particular king of financial instrument, a "prime bank guarantee" which offers a high rate of return. Pyramid schemes again offer high returns for small contributions and invariably collapse leaving the last to join without prospect of recovering any funds.
b) Hacking in the generally recognised sense of unauthorised access and unauthorised modification to computers.
c) Manipulation of computer systems to obtain money from an employer or a third party. Examples of this are diversion of payments and creation of false employees/suppliers.
d) Theft and/or destruction of confidential and sensitive information: This is an area where huge damage can be caused by employees and third parties who are able to gain access to confidential and sensitive information and pass it on to competitors or simply destroy it.
e) Abuse of computer systems by employees. This involves an employee using the computer system for his or her own purposes.
f) Software piracy by either using counterfeit or unlicensed software or by distributing counterfeit software by disk, CD or through the Internet.

2. Why should business take computer fraud seriously:

i) Growing importance of computers / internet / ecommerce in business
ii) Different from conventional frauds in following ways:
   a) Easily hidden and hard to detect.
   b) Difficult to present computer crime to court
   c) Easily committed
iii) General lack of knowledge about how computer works and how systems can be protected

3. Primary Risks to Business

Internal threats:

There is evidence that internal fraud is a greater risk to business than external fraud. A survey conducted in May 1996 found that 4/5 of most serious frauds are committed by employees while 1/5 by collusion between employees and outsiders.

a. Input: The simplest and most common way to commit a fraud is to alter computer input, it requires little, if any, computer skills.
   (i) Collusive fraud
   (ii) Disbursement frauds the perpetrator causes a company either pay too much for ordered goods or to pay for goods that were never ordered.
   (iii) Payroll frauds the perpetrator can enter data to increase that salary, create a fictitious employee, or retain a terminated employee on the records.
   (iv) Cash receipts fraud the perpetrator hides the theft by falsifying system input.
b. Processor: Computer frauds can be committed through unauthorised system use including the theft of computer time and services.
c. Computer Instructions: Computer fraud can be accomplished by tampering with the software that processes company data. This may involve modifying the software, making illegal copies, or using it in an unauthorised manner.

d. Data: Computer fraud can be perpetrated by altering or damaging a company's data files or by copying, using, or scratching them without authorisation. Data can also be destroyed, changed, or defaced-particularly if stored on a company web site.
e. Output: Computer fraud can be carried out by stealing or misusing system output.
f. Malicious alterations of email:

External threats:

- Removal of information
- Destruction of system integrity
- Interference with web pages
- Transmission of viruses by email
- Interception of email
- Interception of electronic payments

4. Internet Frauds

- There are a number of characteristics of the Internet, which are likely to attract fraudsters seeking to make easy money from gullible victims.
- It is unregulated in so far as who may set up a site.
- An Internet site can be set up anywhere in the world at very low cost and can reach anywhere else in the world at low cost.
- An impressive site with links to established companies or financial institutions may be no more than an empty shell designed to attract and trap the unwary.
- A site may, and probably will, operate outside the legal jurisdiction of the country in which the victim of the fraud resides.

5. Computer Fraud and Abuse Techniques

Technique	Description
Cracking	Unauthorized access to and use of computer systems usually by means of a personal computer and a telecommunications network. Crackers are hackers with malicious intentions.
Data diddling	Changing data before during or after it is entered into the system in order to delete, alter, or add key system data.
Data leakage	Unauthorised copying of company data such as computer files.
Denial of service attack	Attacker sends e-mails bombs (hundreds of messages per second) from randomly generated false addresses. Internet service provider's e-mail is overloaded and shuts down.
Eavesdropping	Listening to private voice or data transmissions often using a wiretap.
E-mail forgery	Sending an e-mail message that looks as if it were sent by someone else
E-mail threats	Sending a threatening message to try and get recipient to do something that would make it possible to defraud him.
Hacking	Unauthorised access to and use of computer systems, usually by means of a personal computer and a telecommunications network. Hackers do not intend to cause any damage.

Internet misinformation	Using the internet to spread false or misleading information about companies.
Internet terrorism	Using the Internet to disrupt electronic commerce and to destroy company and individual communications.
Logic time bomb	Program that lies idle until some specified circumstance or a particular time triggers it. Once triggered the bomb sabotages the system by destroying programs, data, or both.
Masquerading or impersonation	Perpetrator gains access to the system by pretending to be an authorized user.Enjoys same privileges as the legitimate user.
Password Cracking	Intruder penetrates a system`s defenses, steals the file containing valid passwords, decrypts them, and then uses them to gain access to system resources such as programs, files, and data.
Piggybacking	Tapping into a telecommunications line and latching on to a legitimate user before he logs into the system, legitimate user unknowingly carries perpetrator into the system.
Round-down	Computer rounds down all interest calculations to two decimals places. Remaining fraction of a cent is placed in an account controlled by perpetrator.
Salami technique	Tiny slices of money are stolen over a period of time. (Expenses are increased by a fraction of a percent; increments are placed in a dummy account and later pocketed by the perpetrator.)
Scavenging	Gaining access to confidential information by searching corporate records. Scavenging methods range from searching trashcans for printouts or carbon copies of confidential information to scanning the contents of computer memory.
Social engineering	Perpetrator tricks an employee into giving out the information needed to get into a system.
Software piracy	Copying computer software without the publisher`s permission.
Spamming	E-mailing the same message to everyone on one or more usenet news groups or LISTSER V lists.
Super zapping	Unauthorised use of special system programs to bypass regular system controls and perform illegal acts.
Trap door	Perpetrator enters the system using a back door that bypasses normal system and controls and perpetrates fraud.
Trojan horse	Unauthorised computer instructions in an authorized and properly

	functioning program
Virus	Segment of executable code that attaches itself to software replicates itself, and spreads to other systems or files. Triggered by a predefined event, a virus damages system resources or displays a message on the monitor.
War dialing	Programming a computer search for an idle modern by dialing thousands of phone lines. Perpetrator enters the system through the idle modem. Captures the personal computer attached to the modem.
Worm	Similar to a virus except that it is a program rather than a code segment hidden in a host program. A worm also copies and actively transmits itself directly to other systems. It usually does not live very long, but it is quite destructive while it is alive.

6. Preventing Computer Frauds

Prevention:

(i) Security measures: Employees should be well-schooled in security measures, taught why they are important, and motivated to take them every seriously.
(ii) Telephone disclosures: Employees should be taught to not give out confidential information over the telephone without knowing for sure who is calling.
(iii) Fraud awareness: Employees should be made aware of fraud, its prevalence, and its dangers.
(iv) Ethical considerations: The Company should promote its ethical standards in its practices and through company literature such as employee handouts.
(v) Punishment for unethical behaviour: Employees should be informed of the consequences of unethical behaviour.
(vi) Educating employees in security issues, fraud awareness, ethical considerations and the consequences of choosing to act unethically can make a tremendous difference.
(vii) Manage and Track Software Licenses:
(viii) Require Signed Confidentially Agreements: All employees vendors, and contractors should be required to sign and abide by a confidentiality agreement.

Increase the difficulty of committing fraud:

(i) Develop a Strong System of Internal Controls: The overall responsibility for a secure and adequately controlled system lies with top management.
(ii) Segregate Duties:
(iii) Require Vacations and Rotate Duties
(iv) Restrict Access to Computer Equipment and Data Files
(v) Encrypt Data and Programs
(vi) Protect Telephone Lines
(vii) Protect the System from Viruses
(viii) Control Sensitive Data
(ix) Control Laptop Computers

Improve Detection Methods:

(i) Conduct Frequent Audits
(ii) Use a Computer Security Officer
(iii) Use Computer Consultants
(iv) Monitor system Activities
(v) Use Fraud Detection Software

7. Rise in Computer frauds

2. Not everyone agrees on what constitutes computer fraud.
3. Only 1% are detected.
4. 80% to 90% are not reported.
5. Low level of security
6. Many sites give step by step instructions on how to perpetrate fraud.
7. Law enforcement unable to keep up with growing number of frauds.

8. Reduce Fraud Losses

No matter how hard a company tries to prevent fraud, chances are that it will occur.
Maintain adequate insurance.
Keep a current backup copy of all program and data files in a secure off-site location.
Develop a contingency plan for fraud occurrences and other disasters that might occur.
Use special software designed to monitor system activity and help companies recover from frauds and malicious actions.

9. Detection of Computer Frauds:

Disk imaging and analysis Technique:

(i) An exact copy of the computer hard disk is taken leaving the original completely intact and leaving no trace of the copying process.

(ii) The image copy of the disk is processed and areas of storage containing partially overwritten files and files which have been marked as deleted but not overwritten are recovered.

10. SECURITY IN CASE OF PERSONAL COMPUTERS

Due to some of their peculiar characteristics personal computers face some additional security risks. These computers are small, available in many makes, are prone to virus infection, use ready-made packages etc. Hence the risk in their case is:

They can be and are shifted from location to location
Decentralised purchasing of PC's may result in hardware/software incompatibility
Floppies are handled and shifted and hence corrupt rapidly
Segregation of duties is not possible
They are prone to computer viruses
Absence of trained staff

The possible security measures that be taken are:

Physically locking the PC or the keyboard
Centraliazed coordination of PC purchase.
Floppies to be stored in secured places.
Regular backups to be taken
Unauthorized software should not be used.
Regular training to be intimated.

Year of Exam	Question No.	Chapter No.	Ans. Page No.	Marks	Question
Nov-02	[6(a)]	15	15.15-15.16	10	What measures can be adopted to detect Computer Frauds?
May-03	[7(c)]	15	15.17-15.18	5	Write short note : Disc Imaging and analysis Technique

Nov-03	[5(c)]	15	15.3-15.4	10	Why should businesses take Computer Frauds seriously?
May-04	[4(c)]	15	15.4	5	What are the computer frauds committed through input?
May-04	[7(a)]	15	15.6-15.7	5	Write short note : Internet frauds
Nov-04	[6(a)]	15	15.7 - 15.9	10	Substantiate with reasons to the view that there is a steep rise in the Internet Computer fraud. Why many institutions are unable to contain it?
May-05	[1(c)]	15	15.3-15.4	5	Why is Computer fraud a serious threat to any business organisation?
May-05	[7(d)]	15	15.17-15.18	5	Write short notes on: Disc Imaging and Analysis Technique.
Nov-05	[5(a)]	15	15.13-15.15	10	What kind of controls can be incorporated in the system to make frauds difficult to perpetrate?
May-06	[1(d)]	15	15.9-15.11	5	Define the following computer Fraud and Abuse techniques. (i) Hacking (ii) Logic time bomb (iii) Piggy backing (iv) Spamming (v) Data didding
Nov-06	[4(c)]	15	15.4-15.5	5	How can computer fraud be committed using input in four different ways?
Nov-06	[7(d)]	15	15.6-15.7	5	Internet Frauds
May-07	[4(c)]	15	15.15-15.16	5	What steps can be taken to detect computer fraud?
Nov-07	[5(c)]	15	15.4-15.6	5	Briefly explain five categories of Computer frauds based on the data processing model.
May-08	[3(b)]	15	15.13-15.15	10	Briefly explain various kinds of controls that can be incorporated in the system to make frauds difficult to perpetrate.
May-08	[4(c)]	15	15.9-15.11	10	Define the following computer fraud and abuse technique: (i) War dialing (ii) Scavenging (iii) Cracking (iv) Internet terrorism (v) Masquerading.
Nov-08	[1(c)]	15		8	Recently you have received a report from your bank client that money from one account has been unauthorisedly transferred to another account by stealing the login information of a client through Internet. How will you stop the recurrence of such events?

Chapter XVI: *CYBER LAWS AND INFORMATION TECHNOLOGY ACT 2000*

I. Brief History

The Government of India realized the need for introducing a new law and for making suitable amendments to the existing laws to facilitate **e-commerce and give legal recognition to electronic records and digital signatures.**

II. Objectives of the Act

1. To grant legal recognition to transactions carried out by means of EDI and other means of electronic communication commonly referred to as e-commerce in place of paper based methods of communication.
2. To grant legal recognition to Digital signature for authentication of any info. or matter which requires authentication under any law for time being in force.
3. To facilitate electronic filing of documents with Government Departments
4. To facilitate electronic storage of data.
5. Facilitate and give legal recognition to fund transfer between banks and financial institutions.
6. Legal recognition for keeping books of account by Bankers in electronic form.
7. To amend Indian penal code, Indian evidence Act, Banker's Book Evidence Act and RBI Act.

III. Scope of the Act and Definitions

It extends to the whole of India and unless otherwise provided in the Act, it applies to any offence or contravention there under committed outside India by any person.

The Act shall not apply to following:

1. A negotiable instrument (other than cheque) as defined in negotiable instrument Act, 1881.
2. Power of Attorney as defined in P-O-A Act, 1882.
3. A trust as defined in Indian Trusts Act, 1882.
4. A will as defined in Indian Succession Act, 1925 including any other testamentary disposition by whatever name called.
5. Any contract for sale or conveyance of immovable property or any interest in such property.
6. Any such class of documents or transactions as may be notified by Central Government in official Gazette.

Important Definitions

(i) Addressee
(ii) Afixing digital signature
(iii) A symmetric Crypto System
(iv) Digital signature
(v) Electronic form
(vi) Information
(vii) Intermediary
(viii) Key pair
(ix) Originator
(x) Prescribed
(xi) Private key
(xii) Public Key

IV Authentication of Electronic Records using Digital Signatures

The digital signature is created in two distinct steps. First the electronic record is converted into a message digest by using a mathematical function known as hash function which digitally freezes the electronic record thus ensuring the electronic record thus ensuring the integrity of the content of the intended communication contained in the electronic record. Any tampering with the content of the electronic record will immediately invalidate the digital signature.
Secondly, the identity of the person affixing the digital signature is authenticated through the use of a private key which attaches itself to the message digest and which can be verified by anybody who has the public key corresponding to such private key.
This will enable anybody to verify whether the electronic record is retained intact or has been tampered with since it was so fixed with the digital signature.
It will also enable a person who has a public key to identify the originator of the message.
Refer Annexure 1

V Electronic Governance

It specifies the procedures to be followed for sending and receiving of electronic records.

S.	Title	Content
4	Legal recognition of electronic records	Where any law requires that any information or matter should be in the typewritten or printed form then such requirement shall be deemed to be satisfied if it is in an electronic form.
5	Legal recognition of Digital Signatures	Where any law requires that any information or matter should be authenticated by affixing the signature of any person, then such requirement shall be satisfied by means of Digital Signature affixed in such manner as may be specified by Central Government.
6	Foundation of Electronic Governance	It provides that filling of any form, application or other documents, creation, retention or preservation of records, issues or grant of any license or permit or receipt or payment in Government offices and its agencies may be done through the means of electronic form. The appropriate Government has the power to prescribe the manner and format of the electronic records and the method of payment of fee in that connection.
7	Documents to be retained in electronic form	It provides that the documents, records or information which has to be retained for any specified period shall be deemed to have been retained if the same is retained in the electronic form provided the follow provided the following conditions are satisfied: (i) the information therein remains accessible so as to be usable subsequently. (ii) The electronic record is retained in its original format or in a format which accurately represents the information contained. (iii) The details which will facilitate the identification of origin, destination, dates and time of dispatch or receipt of such electronic

		record are available therein.
8	Publication of rules, regulations and notifications in the Electronic Gazette.	It provides that where any law requires publication of any rule, regulation, order, by-law, notification or any other matter in the official gazettethen the requirement shall be deemed to be satisfied if the same is published in an electronic form.
9	CG/SG can't insist doc. to be in electronic form.	It provides that the conditions stipulated in S. 6,7 & 8 shall not confer any right to insist that the document should be accepted in electronic format by CG/SG

Power of Central Government to make Rules (Sec 10)

CG, in respect of Digital Signature may prescribe by rules the following: -

(a) The type of digital signature.
(b) Manner and format in which it has to be a fixed
(c) Manner of procedure which facilities identification of person Afixing digital signatures.
(d) Control processes/procedures, to ensure adequate integrity, security and confidentiality.
(e) Any other matter.

VI Attribution receipts and dispatch of electronic records

11 – How Electronic Record attributed to person who originated it.
12 – Acknowledgement of Receipt.
13 – Time and Place of Dispatch and Receipt.

VII Secure Electronic records and secure digital signatures (Sec 14-16)

Security procedures need to be applied to digital signature for being treated as secure digital signature and CG is empowered to prescribe security procedures after taking into account factors like nature of transaction, level of sophistication availability and cost of alternative procedures etc.

VIII Regulation of Certifying Authorities

A **F**lat **F**rown **R**ed **L**ady **A**rrived **R**ear **R**oad **R**iver (17-25)

Section	Code	Contents
17	A	Appointment of Controller and other officers to regulate certifying authorities.
18	F	Functions of controller i.r.o. Certi. Authorities
19	F	Foreign Certifying Authorities (recognition of)
20	R	Controller acting as Repository of all Digital Signature Certificates. He maintains a computerized database of all public keys in such a manner that they are available to general public
21	L	Power of Controller to issue license to the Certifying Authority to issue Digital Signature Certificates.
22	A	Application for license.
23	R	Renewal of license
24	R	Rejection or Grant of license by controller on certain grounds
25	R	Revocation of license/suspension

27		Controller's power to delegate
30		Duties of Certifying Authorities Certain procedures to be followed i.r.o. Digital Signatures. (URSO) (a) make use of hardware, software, and procedures that are secure from intrusion and misuse; (b) provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions. (c) adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured and (d) observe such other standards as may be specified by regulations. Every person employed by him complies with provisions of Act, Rules, Regulations, etc. Display of license at conspicuous place. Immediate surrender in case of suspension/revocation of license Disclose Digital Signature Certificate which contains public key corresponding. to Pvt. key used by certifying authority.

IX Digital Signature Certification

- Procedure for application
- Procedure for suspension
- Procedure for revocation

Certifying authority must be satisfied that applicant

1. Holds private key corresponding to public key
2. Private key is capable of creating digital signature
3. Public key can be used to verify digital signature affixed.

X Duties of subscribers (40-42)

1. On acceptance of Dig. Signature certificate, the subscriber shall generate key pair using secure system.
   Deemed to have accepted DSC when
   i. Publishes or authorises publication to one or more persons.
   ii. Otherwise demonstrates his approval to DSC
   By so accepting subscriber certifies to the public that –
   i. Holds private key corresponding to public key.
   ii. Info contained in certificate as well as material relevant to them are true.
2. Exercise reasonable care to retain control of his private key corresponding to public key. If it is compromised (endangered or exposed), immediately communicate the fact to certifying Authority, else subscriber shall be liable till he has informed.

XI Penalties and Adjudication

Sec 43 deals with penalty for damage to computer system, etc by any of different methods.

Sec 46 confers the power to adjudicate contravention under the Act to an officer not below the rank of Director to Government of India or equivalent officer of state. Such application shall be made by CG. Person so appointed shall have adequate exp. in field of Info. Technology and such legal and judicial experience as may be prescribed by CG.

Sec 47 provides that while deciding upon the quantum of compensation the adjudicating officer shall have due regards to (i) amt. of gain of unfair advantage. (ii) amt. of loss caused to any person (iii) nature of default.

XII Cyber Regulations Appellate Tribunal

It has appellate powers in respect of orders passed by adjudicating officer.

1. Establishment and composition (no, qualification, period of holding office)
2. Salaries and Allowances
3. Filling of Vacancy
4. Resignation and removal of presiding officer
5. Appeal to Cyber Regulations Appellate Tribunal
6. Powers and procedures of Appellate Tribunal
7. Appeal to High Court.
8. Compounding of Contravention
9. Recovery of Penalty

XIII Offences, Powers and Penalties (65-78)

The **H**ead **O**ffice **D**epartment **I**nternal **P**roblems **M**ade **C**hairman **F**ace **F**ar **I**ntensive **C**ircumstances **I**n **P**ublic.

Section	Code	Contents	Imprisonment Upto	Fine Upto
65	T	Tampering with computer source documents	3 years	Rs. 200,000
66	H	Hacking with computer system publishing of Info. which is 1st time subsequent	3 years	Rs. 200,000
67	O	Obscene in elec. Form	10 years	Rs. 200,000
68	D	Controller's directions to certifying Authorities or any employees failure to comply	3 years	Rs. 200,000
69	I	Intercept any info transmitted through any computer system/network		
70	P	Protected system. Any unauthorised access to such system	10 years	Not Defined
71	M	Penalty for Misrepresentation or suppressing any material fact	2 years	Rs. 100,000
72	C	Penalty for breach of confidentiality and privacy of el. records, books, info., etc without consent of person to whom they belong.	2 years	Rs. 100,000
73	F	Penalty for publishing False Digital Signature Certificate	2 years	Rs. 100,000
74	F	Fraudulent Publication	2 years	Rs. 100,000
75	I	Act also to apply for offences or contravention committed outside India if the act or conduct constituting the offence involves a computer, computer system or computer network located in India		

76	C	Confiscation of any computer, computer system, floppies, CDs, tape drives or other accessories related thereto in contravention of any provisions of the Act, Rules, Regulations or Orders made.		
77	I	Penalty and Confiscation shall not interfere with other punishments provided under any law.		
78	P	Power to investigate offences by police officer not below rank of Dy. Superintendent of Police.		

XIV Network Service Providers Not Liable in Certain Cases.

Shall not be liable for any third party info or data made available by him, if he proves that the offence was committed without his knowledge/consent.

XV Miscellaneous

1. Power of Central Government to make Rules [Sec. 87]
2. Power of State Government to make Rules
3. Cyber Regulations Advisory Committee.
4. Power of the Controller to make Regulations.
   F – Foreign Certifying Authority
   L – Terms and Conditions under which Licence may be granted.
   O – Other Standards to be observed by certifying Authority
   D – Database
   S – Particulars to be submitted for issue for Digital Signature Certificate
   D – Disclosure by Certifying Authority U/s. 34
   C – Communicate compromise of pvt. key to the certifying Authority.
5. Power of Police officer/ other officers to enter, search, arrest etc.
6. Liability of companies [Sec. 85]

Year of Exam	Question No.	Chapter No.	Ans. Page No.	Marks	Question
Nov-02	[5(a)]	16	16.6,16.11	10	What is a Digital Signature? How is it used? What are the duties of certifying authorities in regard to its usage?
May-03	[1(a)]	16	16.2-16.6	10	Explain briefly the scope of the Information Technology act, 2000 along with the relevant definitions that are used.
Nov-03	[7(c)]	16	16.6	4	Write Short Note : Digital Signature Certificate
May-04	[1(a)]	16	16.19-16.20	10	What are the powers of the Central Government to make rules, as given in Section 87, Chapter XIII of Information Technology act, 2000?
Nov-04	[1(b)(i)]	16	16.3	2	Define: (i) Affixing digital signature
Nov-04	[1(b)(ii)]	16	16.4	2	Define: (ii) Asymmetric crypto system
Nov-04	[1(b)(iii)]	16	16.4	2	Define: (iii) Computer network
Nov-04	[1(b)(iv)]	16	16.5	2	Define: (iv) Private and Public keys
Nov-04	[1(b)(v)]	16	16.5	2	Define: (v) Secure system
May-05	[1(b)]	16	16.2	5	State the objectives and scope of IT Act, 2000

Nov-05	[6(c)]	16	16.11	5	What are the duties of certifying authorities with respect to digital signature ?
May-06	[1(b)]	16	16.14-16.16	5	Describe the composition and powers of cyber regulatory appellate tribunal.
Nov-06	[5(a)]	16	16.16	10	Describe some of the powers of the cyber Apllelate Tribunal.
May-07	[5(b)]	16	16.21	5	Describe some of the powers of controller under section 89 to make regulations consistent with Information Technology Act, 2000.
Nov-07	[1(b)]	16	16.11	5	What are the duties of certifying authorities with respect to digital signature ?
Nov-07	[7(a)]	16	16.2	5	Objectives of Information Technology Act, 2000
May-08	[1(d)]	16	16.19-16.20	5	Discuss briefly the powers of Central Government under Section 87 to make rules in respect of Information Technology Act, 2000.
Nov-08	[1(b)]	16	16.14-16.16	4	Describe the composition and powers of cyber regulatory appellate tribunal.
Nov-08	[3(c)]	16	16.7-16.8	5	Discuss the main provisions provided in Information Technology Act, 2000 to facilitate E-governance.

Chapter XVII: *AUDIT OF INFORMATION SYSTEMS*

1. Information Systems auditing is the process of collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity allows organizational goals to be achieved effectively and uses resources efficiently.

2. The goals of asset safeguarding data integrity system effectiveness and system efficiency can be achieved only if organization's management sets up system of internal controls.

3. Control: A control is a system that prevents detects or corrects on unlawful event (Source: Information Systems Control And Audit, Ron Weber).

4. Control objectives: Statements of the desired result or purpose to be achieved by implementing control procedures.

5. Risk: The potential that a given threat will exploit vulnerabilities of an asset or a group of assets to cause loss of / or damage to the assets. It is usually measured as a combination of impact and probability of occurrence.

6. The audit methods that are effective for manual audits prove ineffective in IS audits because:
   i. Electronic Evidence
   ii. Terminology
   iii. Automated processes
   iv. New Risks and Controls
   v. Reliance on electronic evidence = Adequacy of Controls

7. IS Audit Scope
   i. Computerised systems and applications
   ii. Information processing facilities
   iii. Systems Development
   iv. Management of Information systems
   v. Client / Server, Telecommunications and Intranet

8. Objectives of IS Audit
   IS Auditor should establish control objectives, review audit subject and recommend actions that would provide a reasonable level of control.
   i. Security provisions protect computer equipment, programs, communication and data from unauthorized access, modification, or destruction.
   ii. Program development and acquisition is performed in accordance with management's general and specific authorization.
   iii. Program modifications have the authorization and approval of management.
   iv. Processing of transaction, files, report and other computer record is accurate and complete.
   v. Source data that is inaccurate or improperly authorized is identified and handled according to prescribed managerial policies.
   vi. Computer data files are accurate, complete, and confidential.

9. Framework for audit of Computer Security. (Refer Page 17.6-17.7)

10. Framework for audit of Program Development. (Refer Page 17.8)

11. Framework for audit of Program Modification. (Refer Page 17.10)

12. Framework for audit of Computer Processing. (Refer Page 17.13)

Test Data Processing:

One way to test program is to process a hypothetical series of valid and invalid transactions. The program should process all of the valid transactions correctly and identify and reject all of the invalid ones. All logic paths should be checked for proper functioning by one or more of the test transactions.

Several resources are available when preparing test data. For Example :

- A listing of actual transactions.
- The test transactions that the programmer used to test the program.
- A **test data generator program**, which automatically prepares test data based on program specifications.

Concurrent Audit Techniques:

The Auditor uses concurrent audit techniques to continually monitor the system and collect audit evidence while live data are processed during regular operating hours. Concurrent audit techniques use embedded audit modules, which are segments of program code that performs audit functions.

i) **An integrated test facility (ITF):** technique places a small set of fictitious records in the master files. The records might represent a fictitious division department. For example auditors could use ITF in the following ways: If the application is in the payroll system they might set up fictitious person in the database. Auditors then use test data to update the fictitious entity. Because fictitious and actual records are processed together, company employees usually remain unaware that this testing is taking place. The system must distinguish ITF records from actual record collection information on the effects of the test transactions, and report the results. ITF is well suited to testing on-line processing systems because test transactions can be submitted on a frequent basis, processed with actual transactions and traced throughout every processing stage.

ii) **The snapshot technique:** The snapshot technique involves having software take "pictures" of a transaction as it flows through an application system at those points where they deem material processing occurs. The embedded software then captures images of a transaction as it progresses through these various processing points. To validate processing at the different snapshot points, auditors usually have the embedded software capture both before images and afterimages of the transaction. They then can assess the authenticity, accuracy, and completeness of the processing carried out on the transaction by scrutinizing the before image, the afterimage, and the transformation that has occurred on the transaction.

iii) **SCARF (system control audit review file):** Audit modules to continuously monitor transaction activity and collect data on transactions with special audit significance. The data are recorded in a SCARF file or audit log. Transactions that might be recorded in a SCARF file include those exceeding a specified rupee limit, involving inactive accounts, deviating from company policy, or containing write-downs of asset values.

iv) **Audit hooks:** are audit routines that flag suspicious transaction. For example. Internal auditors at an insurance Company determined that their policyholder system was vulnerable to fraud every time a policyholder changed his or her name or address and then subsequently withdrew funds from the policy. When audit books are employed auditors can be informed of questionable transactions as soon as they occur.

v) **Continuous and intermittent simulation (CIS):** embeds an audit module in a data base management system. If a transaction has special audit significance, the module independently processes the data (in a manner similar to parallel simulation), records the results, and compares them with those obtained by the DBMS.

Analysis of Program Logic:

If an auditor suspects that a particular application program contains unauthorized code or serious errors, a detailed analysis of the program logic may be necessary.

- **Automated flowcharting programs,** which interpret program source code and generate a corresponding program flowchart.
- **Automated decision table programs,** which generate a decision table representing the program logic.
- **Scanning routines,** which search a program for occurrences of specified variable name or other character combinations.
- **Mapping programs,** which identify unexecuted program code.
- **Program tracing,** which sequentially prints all application program steps (line numbers or paragraph names) executed during a program run)

13. Framework for audit of Source Data (Refer Page 17.18)

14. Framework for audit of Computer Data files (Refer Page 17.20-17.21)

Year of Exam	Question No.	Chapter No.	Ans. Page No.	Marks	Question
Nov-02	[1(a)]	17	17.14-17.15	10	Describe the majour techniques of Concurrent audit of Information systems. Bring out the relevance of such audit.
May-03	[6(a)]	17	17.1-17.2	10	Discuss the various issues that are of primary concerns for an auditor involved in information system audit.
May-03	[7(b)]	17	17.15	5	Write short note : System Control audit Review File (SCaRF)
Nov-03	[1(c)]	17	17.4	6	While performing an IS audit, the auditor should make sure that various objectives are met. Briefly describe them.
Nov-03	[1(a)]	17	17.4	2	What is the sole purpose of an Information System (IS) audit?
Nov-03	[1(b)]	17	17.4	2	What is the role of an IS auditor?
May-04	[1(b)]	17	17.6-17.7	10	Briefly discuss the frame work on which the auditor should work for the audit of Computer Security.
May-04	[7(b)]	17	17.14-17.15	5	Write short note : Integrated test facility
Nov-04	[1(a)]	17	17.14-17.15	10	"In On-line systems, conventional audit trail is difficult and almost impossible" Why? Explain the kind of audit techniques used in such system.

May-05	[1(a)]	17	17.13	10	Your client has recently switched over from manual accounting to computerised accounting. When you receive computerized accounts for the first quarter you find the following types of error: (i) Incomplete or unauthorized data input (ii) Errors in the files or database during updating (iii) Improper distribution or disclosure of output. You, as an information system auditor, suggest the suitable test of controls for audit of computer processing so that the above mentioned errors can be prevented.
Nov-05	[1(a)]	17	17.2-17.3	5	Discuss various factors that render manual audit method ineffective in IS audit.
Nov-05	[1(b)]	17	17.4	5	Briefly describe the various objectives to be met while performing an IS audit.
May-06	[1(a)]	17	17.18	5	A XYZ company receives orders from customers either by telephone, facsimile or electronic data interchange. A clerk then transcribes the order into one of the company's order from to be keyed into the order entry system. You being the information system auditor of the company, suggest various internal control procedures to be adopted to prevent inaccurate or unathorized source data entry?
Nov-06	[1(d)]	17		5	How does MIS auditing enhance the control process?
Nov-06	[7(b)]	17	17.14-17.15	5	Integrated Test Facility
May-07	[1(d)]	17	17.15-17.17	5	Various software packages serve as aids in analysis of program logic. Explain briefly.
May-07	[7(d)]	17	17.15	5	Snapshot technique
Nov-07	[1(a)]	17	17.4	5	While performing an IS audit, the auditor should ascertain that various objectives are properly met. Briefly describe them.
Nov-07	[7(b)]	17	17.3-17.4	5	Review areas of an IS Auditor
May-08	[1(a)]	17	17.2-17.3	5	Discuss various factors that render manual audit method ineffective in Information System audit.
Nov-08	[1(a)]	17	17.1-17.2	8	Discuss various issues that are of primary concern for an auditor involved in information System Audit.
Nov-08	[6(b)]	17		10	

Persian Paints is a small but highly regarded paint manufacturing company. The company has a network in place linking many of its business operations. Though the firm believes that its security is adequate, the recent addition of a Web site has become an open invitation to hackers. Management requested a risk assessment. The risk assessment identified a number of potential exposures. These exposures, their associated probabilities and average losses are summarized in the following table:

Persian Paints Risk Assessment

	Exposure	Probability of Occurrence(%)	Annual Average Loss(Rs.)
1	Virus attack	60	75,000.00
2	Data Loss	12	70,000.00
3	Embezzlement	3	30,000.00
4	User Errors	95	25,000.00
5	Threats from Hackers	95	90,000.00
6	Improper use by Employees	5	5,000.00
7	Power Failure	15	300,000.00

Using the above risk assessment data, calculate the expected annual loss for each exposure. Which control points have the greatest vulnerability and least vulnerability? Prepare a written report that summarized your findings and recommendations.

Chapter XVIII: *INFORMATION SECURITY*

1. Security Objective:

For any organization, the security objective is met when:

- Information systems are available and usable when required (availability).
- Data and information are disclosed only to those who have a right to know it (confidentiality) and
- Data and information are protected against unauthorized modification (integrity).

The relative priority and significance of availability, confidentiality, and integrity vary according to the data within the information system and the business context in which it is used.

2. Principles of information security

(i) Accountability - Responsibility and accountability must be explicit.
Security of information requires an express and timely apportionment of responsibility and accountability among data owners, process owners, technology providers, and users.

(ii) Awareness - Awareness of risks and security initiatives must be disseminated.
Able to gain knowledge of the existence and general extent of the risks facing the organization and its system and the organization's security initiates and requirements.

(iii) Multidisciplinary - Security must be addressed taking into consideration both technological and non-technological issues.

(iv) Cost Effectiveness - Security must be cost-effective.
Security levels and associated costs must be compatible with the value of the information.

(v) Integration - Security must be coordinated and integrated.
This requires that all levels of the information cycle-gathering, recording, processing, storing, sharing, transmitting, retrieving, and deleting are covered.

(vi) Reassessment - Security must be reassessed periodically
The security of information systems should be reassessed periodically, as information systems and the requirements for their security vary over time.

(vii) Timeliness - Security procedures must provide for monitoring and timely response.
Organizations must establish procedures to monitor and respond to real or attempted breaches in security in a timely manner in proportion with the risk.

(viii) Societal Factors - Ethics must be promoted by respecting the rights and interests of others.
Information and the security of information should be provided and used in such a manner that the rights and interests of others are respected and that the level of security must be consistent with the use and flow of information that is the hallmark of a democratic society.

3. Types of Security Protection

(i) Preventive Information Protection:

This type of protection is based on use of security controls. Information security controls are generally grouped into three types of control: Physical, Logical, and Administrative. Organizations require all three types of controls.

Physical: Doors, Locks, Guards, Floppy Disk Access Locks, Cables locking systems to desks/walls, CCTV, Paper Shredders, Fire Suppression Systems.
Logical (Technical): Passwords, File permissions, Access Control Lists, Account Privileges, Power protection systems.

Administrative: Security Awareness, User Account Revocation, and Policy

(ii) Restorative Information Protection:

Security events that damage information will happen. If an organization cannot recover or recreate critical information in an acceptable time period, the organization will suffer and possibly have to go out of business.

The key requirement of any restorative information protection plan is that the information can be recovered.

Here are a few questions any restorative information protection program must address.

Has the recovery process been tested recently?

How long did it take?

How much productivity was lost?

Did everything go according to plan?

How much extra time was needed to input the data changes since the last backup?

4. Security Policies:

Every organisation should have a security policy that defines acceptable behaviours and the reaction of the organisation when such behaviours are violated. A security policy defines ways in which resources in a computer system may be accessed and used.

a. Policy Development: The security objective and core principles provide a framework for the first critical step for any organization-developing a security policy. Topics addressed may include a statement from the CEO in support of the Information Security policy, importance of information assets, need for security, importance of defining sensitive and critical assets to protect, and accountabilities. Once a policy has been approved by the governing body of the organization and related roles and responsibilities assigned, it is necessary to develop the standards, measures, practices and procedures within which individual systems are then introduced and maintained.

b. Roles and Responsibilities: It is imperative that individual roles, responsibilities, and authority are clearly communicated and understood by all

Executive Management-assigned overall responsibilities for the security of information:

Information System Security Professionals-responsible for the design, implementation, management, and review of the organization's security policy, standards, measures, practices, and procedures.

Data Owners-responsible for determining sensitivity or classification levels of the data as well as maintaining accuracy and integrity of the data resident on the information system.

Process Owners-responsible for ensuring that appropriate security, consistent with the organization's security policy, is embedded in their information systems

Technology providers-responsible for assisting with the implementation of information security

Users-responsible for following the procedures set out in the organization's security policy; and

Information Systems Auditors-responsible for providing independent assurance to management on the appropriateness of the security objectives, and compliance with the organization's security objectives.

c. Design: Once a policy has been approved by the governing body of the organization and related roles and responsibilities assigned it is necessary to develop a security and control framework. The process concludes with the design of an integrated security system that is compatible with the needs of the organization, given technical and cost constraints.

d. Implementation: Once the design of the security standards, measures, practices and procedures has been approved, the solution should be implemented on a timely basis and then maintained.

e. Monitoring: Information systems are subject to a wide range of disruptive incidents of varying degrees of intensity. Preventive measures may not always be feasible or cost-effective to minimize loss, disclosure, damage, or disruption. Hence, monitoring measures need to be established to detect and ensure correction of security breaches, such that all actual and suspected breaches are promptly identified, investigated, and acted upon. This will also ensure ongoing compliance with policy, standards, and minimum acceptable security practices.

f. Awareness, Training, and Education: People are often the weakest link in securing information. Awareness of the need to protect information, training in the skills needed to operate them securely, and education in security measures and practices are of critical importance for the success of an organization's security program. All the employees should be aware of the security policies and its importance should be informed to all the employees on a regular basis.

5. Role of Security Administration:

A security administrator is a person who is solely responsible for controlling and co-ordination activities pertaining to all security aspects of the organisation.

- To ensure that the facilities in which systems are developed, implemented, maintained and operated are safe from threats that affect the continuity of installation and or result in loss of security.
- Sets policy, subject to board approval.
- Investigates, monitors, advice employees, counsels management on matters pertaining to security.
- Establishing the minimal fixed requirements for classification of information based on the physical, procedural, and logical security elements.
- Train security coordinators, select software security packages and solve problems.
- Investigates all security violations
- Advises senior management on matters of information resource control
- Consults on matters of information security
- Conducting a security program, which is a series of ongoing, regular, periodic evaluations of the facilities available.
- Consider an extensive list of possible threats to the organisation, prepare an inventory of assets evaluate the existing controls, implement new controls etc.

Year of Exam	Question No.	Chapter No.	Ans. Page No.	Marks	Question
Nov-02	[5(b)]	18	18.7-18.10	10	What are the core principles of Information Security?
May-03	[1(b)]	18	18.20	10	Explain the role played by an information security administrator.
Nov-03	[6(a)]	18	18.7-18.9	10	Briefly describe any five core principles of Information Security
May-04	[6(a)]	18	18.1-18.2	10	Explain in brief information security and its importance.
Nov-04	[6(b)]	18	18.17 - 18.19	10	Give an e.g.. of an Information Security Policy Statement.
May-05	[2(a)]	18	18.2-18.3	10	What is "Information Security"? State the core principles of Information Security.

May-06	[6(a)]	18	18.12-18.13	10	What do you mean by Information Security policy? Explain the silent features of the Information Security policy
Nov-06	[6(c)]	18		8	Employee Mr. X downloads adult material to his PC at work, and employee Miss Y sees it. Miss Y then proceeds to sue the company for sexual harassment. As the employer, are you liable?
Nov-06	[6(b)]	18		7	Your employees are abusing their internet privileges, but you don't have an internet usage policy. What do you do?
Nov-06	[6(a)]	18		5	Nobody told you that your internet use in the office was being monitored. Now you have been warned you will be fired if you use the internet for recreational surfing again. What are your rights?
Nov-06	[1(a)]	18		5	Why Computerized Information system are more vulnerable to many more kinds of threats than manual systems? Name some of the key areas where large amounts of data stored in electronic form are most vulnerable.
Nov-06	[7(c)]	18	18.11	5	Restorative Information Protection
May-07	[1(b)]	18	18.12-18.13	5	Briefly outline the contents of Information Security policy.
May-07	[7(c)]	18	18.11-18.12	5	Holistic protection
Nov-07	[2(a)]	18	18.1-18.3	10	What is "Information Security"? Why is it important in any organization? Explain briefly
May-08	[6(a)]	18	18.12-18.17	5	Briefly explain the best approach to implement information security policy?
May-08	[6(d)]	18	18.20	5	Briefly explain the role of Information Security Administrator.

Chapter XIX: *USE OF SIMPLE CASE TOOLS, ANALYSIS OF FINANCIAL STATEMENTS USING DIGITAL TECHNOLOGY*

1. What are CASE tools?

CASE Tools are software programs that are designed to assist human programmers with the complexity of the processes and the artifacts of software engineering. They constitute the laws of and the automated tools that aid in the synthesis, analysis, modeling, or documentation of software. In the early eighties, these programs became known as CASE (Computer Aided Software Engineering) Tools.

2. What is Software Engineering?

Software Engineering is the systematic, disciplined and quantifiable approach to the development, operations, maintenance, and retirement of software. It includes the following processes:
translation of user needs into software requirements
transformation of software requirements into design specifications
implementation of design into code
testing of the code for the operational use
documentation.

3. Classification of Case:

A. Tools that support individual process tasks such as checking the consistency of a design, compiling a program, comparing test results and so on.

Tool type	Example
Management tools	PERT tools, estimation tools
Editing tools	Text editors, diagram editors, word processors
Configuration management tools	Version management system, change management system
Prototyping tools	High level language tools, user interface generators
Method support tools	Design editors, data dictionaries, code generators
Language processing tools	Compilers, interpreters
Program analysis tools	Cross reference generators, static analyzers, dynamic analyzers
Testing tools	Test data generators, file compactors
Debugging tools	Interactive debugging system
Documentation tools	Page layout program, image editors
Reengineering tools	Cross reference systems, program restructuring systems

B. Workbenches to support process phases such as specification, design etc. They consist of sets of tools with variable degree of integration.

Components of a Case Work bench:

1. A diagram editing system that is used to create data flow diagrams, structure charts, entity relationship diagrams etc. It captures information about these entities and saves this information in a central repository.
2. Design analysis and checking facilities that process the design and correct errors. These are integrated with the editing system so that the users may be informed of errors during diagram creation.

3. Query language facilities that allow the user to browse the stored information and examine completed designs.
4. Data dictionary that maintains information about named entities in a system design.
5. Report generation facilities that take information from the central store and automatically generate system documentation.
6. Forms generation tools that allow screen and document formats to be specified.
7. Import/export facilities that allow interchange of information from the central repository with other development tools.
8. some system support skeleton code generation which generate code or code segments automatically from the design captured in the central store.

1. Programming work bench:
   Programming work bench is made up of a set of tools to support the process of program development. Some of these tools which are part of a programming work bench are:
   a. Language compiler: Translates host programs to object code. As part of a translation process, an abstract syntax tree and a symbol table is created.
   b. Cross referencer: Produces a cross reference listing showing where all program names are declared and used.
   c. Static analyser: Analyses the source code to discover anomalies such as uninitialized variables, unreachable code, uncalled functions and procedures etc.
   d. Interactive debugger: Allows the user to control the execution sequence and view the program state as execution progresses.
2. 4 GL work benches:
   4GL work benches are geared towards producing interactive application which rely on extracting information from an organizational database.
   a. a database query language such as SQL which may either be input directly or generated automatically from forms filled in by end users.
   b. a form design tool which is used to create forms for data input and display.
   c. a spread-sheet which is used for the analysis and manipulation of numeric information.
   d. A report generator which is used to define and create reports from information in the database.
3. Analysis and design work benches:
   To support the analysis and design stages of the software process where models of the system are created.
   a. Diagram editors to create data flow diagrams, structured charts, entity relationship diagram and son on.
   b. Design analysis and checking tools which process the design and then submit report on errors and anomalies. These are integrated with editing system so that user errors are trapped at an early stage in the process.
   c. Repository query languages which allow the designer to find the designs and associate design information in the repository.
   d. A data dictionary which maintains information about the entities used in a system design.
   e. Report definition and generation tools which take information from the central store and automatically generate system documentation.
   f. Forms definition tools which allow screen and document formats to be specified.
   g. Import-export facilities which allow the interchange of information form the central repository with other development tools.
   h. Code generators which generate code or code skeletons automatically from the design captured in the central store.
4. Testing workbenches

Testing workbenches are open systems which evolve to suit the needs of the system being tested.

The tools which might be included in a testing workbench are:

a. Test manager: Manages the running and reporting of program tests. This involves keeping track of test data, excepted results, program facilities tested and so on.
b. Test data generator: Generates test data for the program to be tested. This may be accomplished by selecting data from a database or by using patterns to generate random data of the correct form.
c. Oracle: Generates predictions of expected results.
d. File Compactor: Compares the result of program tests with previous test results and reports differences between them.
e. Report generator: Provides report definition and generation facilities for test results.
f. Dynamic Analyser: Adds code to a program to count the number of times each statement has been executed.
g. Simulators: Different kinds of simulators such as Target simulators. User Interface simulators. I/O simulators are available for simulation.

5. Meta-CASE workbenches:

Meta case work benches are CASE tools which are used to generate other CASE tools.

There are five different aspects which are to be considered in Meta-case workbench.

a. A data model for data capture and output generation.
b. A frame model which defines the views of the data model to be generated.
c. Diagrammatic notation for each diagram frame.
d. Textual presentation for each text frame
e. Report structures

C. CASE Environment:

A complete CASE environment is a carefully configured and integrated system of automated tools applied to the entire software life cycle for each unique software development, maintenance or redevelopment problem.

D. Analysis of Financial Statements (Refer Page 19.13 – 19.23)

Year of Exam	Question No.	Chapter No.	Ans. Page No.	Marks	Question
Nov-02	[7(b)]	19	19.1,19.3	5	Write short note : CASE tools
May-03	[7(a)]	19	19.11	5	Write short note : Meta-CASE Workbenches
Nov-03	[6(b)]	19	19.1-19.2,19.3-19.4	10	What are CASE Tools? Describe in-depth the categories of CASE tools with examples
May-04	[6(b)]	19	19.15	6	Explain the significance of ratio analysis generally carried out for financial analysis
May-04	[6(c)]	19	19.16	4	Explain briefly the profitability ratio
May-05	[6(c)]	19	19.7-19.8	10	What are called Work benches? Describe the various tools used in programming work bench.
Nov-05	[7(b)]	19	19.9	5	Analysis and design work bench
May-06	[5(c)]	19	19.12	5	Describe briefly five components of CASE work bench.
Nov-06	[5(b)]	19	19.4	5	What are the five different levels of integration on CASE tools?

May-07	[1(c)]	19	19.2-19.3	5	What are CASE Tools? Discuss briefly its three categories.
Nov-07	[3(a)]	19	19.10-19.11	10	Explain with the help of a diagram the various tools which are included in a testing workbench.
Nov-07	[7(c)]	19	19.6-19.7	5	Process Integration
May-08	[1(b)]	19	19.9-19.10	5	Briefly explain the components of an analysis and design work bench.
Nov-08	[7(b)]	19	19.10-19.11	5	Write short note : Testing work benches

APPENDIX

Server-Centric Computing

What is Server-Centric Computing?
Source: http://www.gobiztech.com/serv_servercentric.htm

What is a Digital Signature?

Source: http://www.youdzone.com/signature.html

Questions asked in Previous Examination - Chapterwise

Year of Exam	Q. No.	Chapter No.	Ans. Page No.	Marks	Question
May-03	[2(b)]	1	1.7-1.8	10	Expain the concept of decomposition with the help of an example.
May-04	[7(d)]	1	1.17	5	Write short note : Expert systems
Nov-05	[2(b)]	1	1.10	5	Define the term system stress and system change.
May-06	[2(a)]	1	1.10-1.14	10	What do you mean by Information? Describe the important characteristics of information which makes it useful to the organization.
May-07	[6(c)]	1	1.5	5	Differentiate between open and closed system.
Nov-07	[2(b)]	1	1.15-1.17	10	System analysts develop various categories of information systems to meet a variety of business needs. Discuss any three such systems briefly.
May-08	[7(a)]	1	1.5-1.6	5	Write short note: Closed and open systems.
Nov-08	[7(d)]	1	1.17	5	Write short note : Expert systems.
May-07	[5(c)]	2	2.1	5	What is Transaction processing cycle? Discuss briefly four common cycles of a business activity.
Nov-02	[2(a)]	3	3.16-3.18	8	Differentiate among Strategic, Tactical and Operationalcategories of Information required for different levels ofManagerial decision-making.
May-03	[2(a)]	3	3.9-3.11	10	Discuss the effect of applying computer technology to Management Information System.
Nov-03	[2(b)(i)]	3	3.14-3.15	3	Describe briefly three levels of Management
Nov-03	[2(b)(ii)]	3	3.16,3.17,3.18	6	Mention atleast two pieces of information-one internal and one external-required at every one of the levels of Management.
May-04	[2(c)]	3	3.12-3.13	10	Explain three board categories of the planning information requirements of executives.
Nov-04	[7(a)]	3	3.14 - 3.15	5	Write short note : Strategic and Tactical decisions
May-05	[2(c)]	3	3.6-3.8	5	Describe the main pre-requisites of a Management Information System which makes it an effective tool.
May-06	[1(c)]	3	3.11	5	Discuss the limitations of the management Information System.
Nov-06	[2(a)]	3	3.4-3.6	10	State the factors to be considered for designig the effective Management Information System.
May-08	[2(b)]	3	3.6-3.8	10	Describe the main prerequisites of a MIS which makes it an effective tool. Explain the major constraints in operating it.
May-08	[7(b)]	3	3.13-3.14	5	Write short note: Programmed decisions.
Nov-08	[5(c)]	3	3.8	10	XYZ company engaged in manufacturing and installing power plant equipments has installed a new MIS and you have been requested to evaluate its effectiveness. On what parameters would you evaluate the MIS system?
May-03	[3(b)]	4	4.8-4.9	10	Disucss various benefits which are attained by implementing a computerized model for making decision.
May-03	[7(d)]	4	4.24	5	Wtite short note : Materials Requirement Planning (MRP)

Nov-03	[2(a)]	4	4.13-4.14	8	Explain the role played by Financial Information System in making financial decisions.
Nov-03	[2(b)(iii)]	4	4.9-4.10	3	Discuss the potential impact of computers and MIS at the top level of Management.
May-04	[5(a)]	4	4.24	2	"The Personnel information system is the backbone of any organisation" Explain
May-04	[5(b)]	4	4.25-4.27	6	Discuss various sub-systems of PIS, which are responsible to increase its operational efficiency.
Nov-04	[2(a)]	4	4.22	10	What are the production information requirements of a GM (Production and Operations Management) with regard to production planning and control?
Nov-04	[2(b)]	4	4.27	5	What are the variables that the top management should consider during negotiations with the labour unions?
May-05	[4(a)]	4	4.14-4.19	10	A Company is planning to introduce a new range of products. The top management is advised to get developed on marketing information system which can enhance the decisional capacities in various marketing activities. You being in-charge of this project suggest what information sub-systems are required to developed.
Nov-05	[2(a)]	4	4.1-4.3	10	How systems approach can be used for solving problems ?
May-06	[2(b)]	4	4.19-4.20	5	"Information is necessary to executive for performing the function of planning" Substantiate the above statement with regard to information requirements of marketing system.
May-06	[2(c)]	4	4.13-4.14	5	Describe various decisions which can be made with the help of financial information system.
May-06	[7](iii)	4	4.24	5	Write Shot notes on any four of the following: (iii) Material requirements planning
Nov-06	[2(b)]	4	4.15-4.16	10	Enumerate various information which are required for sales support and sales analysis.
Nov-07	[1(c)]	4	4.8-4.9	5	Discuss any five benefits whicha are attatined by implementing a computerised model for making decisions.
May-08	[5(c)]	4	4.24-4.25	5	“Personnel information system deals with flow of information relating to people.” Explain.
Nov-08	[3(a)]	4	4.11-4.14	10	What is Financial decision making? Which Financial decisions are made with the help of Financial information system?
Nov-02	[2(b)]	5	5.15-5.16	12	In what ways does an Executive Information System differ from the Traditional Information System?
Nov-02	[7(c)]	5	5.2	5	Write short note : Decision Support Systems
Nov-03	[7(a)]	5	5.15-5.16	4	Write Short Note : Executive Information Systems
Nov-04	[2(c)]	5	5.13 - 5.14	5	Successful executives take decisions relying more on intuition than on any quantitative analytical decision technique. Mention five characteristics of the types of information that are responsible for this phenomenon in executive decision-making.
May-05	[2(b)]	5	5.2-5.5	5	"A decision support system supports the human decision-making process rather than providing a means to replace it". Justify the above statement by stating the characteristics of decision support system.

Nov-05	[3(a)]	5	5.15-5.16	10	What is an Executive Information System? Dicuss its various purposes.
May-06	[3(b)]	5	5.7-5.10	5	Describe various software tools used in Decision support system.
May-07	[3(b)]	5	5.10-5.11	10	"Decision support systems are widely used as part of an Organisation's Accounting Information system". Give examples to support this statements.
Nov-07	[6(c)]	5	5.17-5.18	5	Briefely explain the principles to guide the design of measures and indicators to be included in EIS.
May-08	[4(b)]	5	5.5-5.7	5	Briefly discuss four basic components of Decision Support System.
Nov-08	[5(a)]	5	5.15-5.16	5	What is Executive Information System (EIS)? How does EIS differ from Traditional Information Systems?
Nov-02	[3(a)]	6	6.9	8	Explain the major categories of risks involved from the mainframe Computers to client servers?
May-03	[6(b)]	6	6.3, 6.5	10	What is client/ server? Describe the various characterstics that reflect the features of a client/ server/ server system.
Nov-03	[3(a)]	6	6.7-6.8	8	Describe the various components of Client-Server architecture
May-04	[5(c)]	6	6.3, 6.4	12	What is client/ server technology? Enumerate any six of its benefits.
Nov-04	[3(a)]	6	6.7 - 6.8	2	Define a 2-tier and 3-tier architecture.
Nov-04	[3(b)]	6	6.8	8	What are the control techniques to be checked to ensure security for client/ server technology?
Nov-04	[3(c)]	6	6.9	10	Describe four categories of risks that are to be considered during the transaction from the mainframe (or PC) to client/server.
May-05	[7(c)]	6	6.3	5	Write short notes on: Client-server model
Nov-05	[7(a)]	6	6.10-6.11	5	Server - centric model
May-06	[3(c)]	6	6.7-6.8	5	Describe various components of clients server architecture.
May-07	[6(b)]	6	6.8	5	What are control techniques that are essential for the security of the client/server environment?
May-08	[5(b)]	6	6.9	5	Briefly explain the risks associated with client / server model.
Nov-08	[4(b)]	6	6.8	5	What control techniques can be utilized for increasing security in a client-server model?
Nov-02	[3(b)]	7	7.8-7.9	8	Describe the steps involved in prototyping for Systems development.
Nov-02	[3(c)]	7	7.9-7.10	4	If you are the Project Manager of a Software Company with the responsibility for developing a break-through product, combining state of the art hardware and software, will you opt for prototyping as a process model for a product meant for the intensely competitive entertainment market?
Nov-02	[7(a)]	7	7.39 - 7.40	5	Write short note : Data Dictionary
May-03	[3(a)]	7	7.29	10	Describe briefly four categories of the major tools that are used for system development.
Nov-03	[3(b)]	7	7.5-7.6	12	Bring out the reasons as to why the organizations fail to achieve their Systems Development Objectives?

May-04	[2(a)]	7	7.14-7.15	2	What is a system development Life-cycle ?
May-04	[2(b)]	7	7.8-7.9	8	Discuss the four steps of the prototyping approach in system development
Nov-04	[7(d)]	7	7.1 - 7.4	5	Write short note : System Develoment Life-cycle.
May-05	[4(b)]	7	7.25-7.27	5	Describe any five functional areas of a system which needs to be analyzed by system analyst for detailed investigation of the present system.
May-05	[7(b)]	7	7.39	5	Write short notes on: Data dictionary
Nov-05	[2(c)]	7	7.24-7.25	5	What are the fact finding techniques used by a system analyst?
Nov-05	[6(a)]	7	7.22-7.23	10	What are the various Tangible and Intangible benefits that can result from the development of a compurised system ?
May-06	[3(a)]	7	7.25-7.27	10	A company is offering a wide range of products and services to its customers. It relies heavily on its existing information system to provide up to date informaion. The company wishes to enhance its existing systems. You being an Information System auditor, suggest how the investigation of the present information system should be conducted so that it can be further improved upon.
May-06	[7](ii)	7	7.11	5	Write Shot notes on any four of the following: (ii) Top down approach of system development.
Nov-06	[3(a)]	7	7.13-7.14	10	What are the project management items associated with an I.T. project system failures? Give the elements to be included in the adopted framework to avoid such failures.
May-07	[5(a)]	7	7.7-7.10	10	What is prototyping approaches to systems deveplopment? Describe its advantages and disadvantages also.
May-07	[7(a)]	7	7.39-7.40	5	Data dictionary
Nov-07	[1(d)]	7	7.24-7.25	5	Briefly explain the various fact finding techniques which are used by the system analyst for determinig the needs of an organization.
Nov-07	[4(b)]	7	7.2-7.4	5	Discuss the various activitites which are part of the system development life cycle.
Nov-07	[7(d)]	7	7.10-7.11	5	End user development appraoach in system development
May-08	[3(a)]	7	7.25-7.27	10	Discuss in detail, how the investigation of present system is conducted by the system analyst.
Nov-08	[2(b)]	7	7.28-7.29	10	State main objectives of system development tools. Briefly describe the major categories of documentation tools that are used for system development with any one simple illustrative example for each.
Nov-02	[6(b)]	8	8.14-8.15	10	What are the majour factors to be considered in designing User inputs? Explain.
Nov-03	[7(b)]	8	8.26-8.27	4	Write Short Note : System Manual
May-04	[3(a)]	8	8.3-8.4	10	What are the six important factors which should be considered while desiging the user outputs?
May-05	[3(a)]	8	8.3-8.4	10	What are the factors considered to design the ideal layout of a printed output?
May-05	[5(c)]	8	8.18-8.19	5	Discuss the desired characteristics of a good coding system.

Nov-05	[3(b)]	8	8.14-8.15	10	Discuss various issues that should be considered while desiging system input.
May-06	[6(c)]	8	8.15-8.18	5	Suggest suitable guidelines to be followed for efficient form design.
Nov-06	[3(b)]	8	8.19-8.22	5	Discuss some of the commonly used coding schemes.
May-07	[4(a)]	8	8.26-8.27	10	What is system manual? What information is included in it?
Nov-07	[4(c)]	8	8.8-8.9	5	State the standards to be followed while designing graphical output
May-08	[5(a)]	8	8.14-8.15	5	Discuss various issues that should be considered while designing system input.
Nov-08	[4(c)]	8	8.18-8.19	5	What are the characteristics of good coding scheme for data input?
May-03	[4(a)(i)]	9	9.4	2	What is an application software?
May-03	[4(a)(ii)]	9	9.4	4	Enumerate the advantages of prewritten application software packages.
May-03	[4(a)(iii)]	9	9.3-9.4	4	Dicuss the factors upon which "Make or Buy" decisionof an application software depends.
Nov-03	[7(d)]	9	9.10-9.11	4	Write Short Note : Point Scoring analysis in Vendor Evaluation
May-04	[3(b)]	9	9.18-9.21	10	Describe any five program design tools.
Nov-04	[4(a)]	9	9.4 - 9.5	5	List the various sources of acquiring the software.
Nov-04	[4(b)]	9	9.4	5	Discuss four most compelling advantages of using a pre-written application package.
May-05	[3(b)]	9	9.6-9.7	10	What is Vendor evaluation? Define the process for the same.
Nov-05	[4(a)]	9	9.13-9.18	10	Discuss various stages through which an in-house creation of program has to pass.
Nov-05	[6(b)]	9	9.4	5	What are the advantages of using pre-written application packages?
May-06	[4(b)]	9	9.6-9.7	5	Briefly discuss about various factors which should be considered for evaluating the vendor proposal for supply of computer system.
May-06	[7](v)	9	9.4-9.5	5	Write Shot notes on any four of the following: (v) Sources pf packaged software
Nov-06	[3(c)]	9	9.12-9.13	5	Discuss Bench marking problem on vendor's proposal.
May-07	[2(a)]	9	9.13-9.18	10	State and briefly explain the various stages of developing an inhouse program.
Nov-07	[5(a)]	9	9.18-9.21	10	Briefly discuss any five program design tools.
Nov-07	[6(b)]	9	9.5	5	State the steps involved in selection of computer systems.
May-08	[5(d)]	9	9.21-9.22	5	Briefly describe various steps involved in system testing.
May-08	[7(c)]	9	9.16-9.17	5	Write short note: Program documentation.
Nov-08	[4(a)]	9	9.2-9.3, 9.11	10	Discuss in brief salient features of consideration while selecting a computer system. Also suggest contents in a point scoring table for evaluation of a ready to use software.
Nov-02	[7(d)]	10	10.10-10.11	5	Write short note : System Maintenance
May-03	[5(a)]	10	10.2-10.3	10	Why is personnel training important for the successful implementation of information system? What type of training should be imparted to (i) systems operator and (ii) users

Nov-03	[4(a)]	10	10.4-10.5	5	Explain the different conversion strategies used for conversion from a manual to a computerized system.
Nov-03	[4(b)]	10	10.4	3	Discuss briefly the advantages and disadvantages of any one conversion strategy.
Nov-04	[4(c)]	10	10.9 - 10.10	10	"The final step of the system implementation is its evaluation." What functions are being served by the system evaluation ? Discuss development,operation and information evaluations.
May-05	[5(b)]	10	10.5-10.8	5	Explain different activities involved in conversion from manual system to computerized system.
Nov-05	[7(d)]	10	10.10-10.11	5	System maintence
May-06	[4(c)]	10	10.4-10.5	5	Describe various stratergies for change over from manual system to computerised.
Nov-06	[4(b)]	10	10.2-10.3	5	Why is personnel training important? What type of training should be imparted to users?
May-07	[6(a)]	10	10.1-10.2	10	Describe various steps that should be taken for successful installation of the equipment during the implementation phase.
May-07	[7(b)]	10	10.10-10.11	5	System maintenance
Nov-07	[4(a)]	10	10.5-10.9	10	Explain briefly various activities that should be completed for successful conversion of an existing system to the new information system.
May-08	[6(b)]	10	10.9-10.10	5	What is the purpose of the system evaluation? How is it performed?
Nov-08	[5(b)]	10	10.10-10.11	5	Define and differentiate between 'Scheduled maintenance' and 'Rescue maintenance' along with their respective benefits.
Nov-02	[4(b)]	11	11.46	6	Draw a system flow chart for a Production Scheduling system.
Nov-02	[4(c)]	11	11.46-11.47	4	What systems interfaces are involved in Production Planning?
May-03	[5(b)]	11	11.16-11.17	10	Draw a payroll flow chart explaining the processes involved.
Nov-03	[4(c)]	11	11.36,11.37,11.38	12	For a material inventory control system, draw the system flowchart and explain the following: System interfaces, Files and inputs, Reports
Nov-04	[5(b)]	11	11.32 - 11.33	5	What do your understand by ON-LINE, REAL-TIME SYSTEMS?
Nov-04	[5(c)]	11	11.34	5	For an On-line, Real-time sale order processing system, draw the systems flow chart.
May-06	[4(a)]	11	11.46-11.47	10	What do you mean by production scheduling? Draw the information flow diagram for design of computerized sxheduling system. Also Explain: (i) System interface ii) File inputs and iii) Reports required for the above systems
Nov-06	[4(a)]	11	11.33-11.35	10	Describe the sequences of events which occur immeadiately for each transaction when controlled by the sales order entry computer programs in OLRT system.
May-07	[3(a)]	11	11.51-11.52	10	What is share accounting system? Describe briefly the input, outputs and processing steps involved in this system.

Nov-07	[3(b)]	11	11.36-11.37	10	What do you understand by Material Inventory Control System? Draw the Information flow diagram for designing computerized material inventory control system.
May-08	[2(a)]	11	11.40-11.42	10	What is work-in-process control system? Describe briefly the system interfaces, files and inputs, and reports involved in this system.
Nov-08	[2(a)]	11	11.13-11.17	10	What is Payroll accounting? Describe in brief the inputs and master file, output and system flow diagram required for it.
Nov-02	[4(a)]	12	12.2,12.5,12.17	10	What is an ERP system? Bring out the major challenges involved in its implementation
May-03	[4(b)]	12	12.14-12.15	10	Explain the process of evaluation of various ERP packages.
Nov-03	[5(a)]	12	12.2	2	What is an ERP (Enterprise Resource Planning) system?
Nov-03	[5(b)]	12	12.16	8	Write down the general guidelines which are to be followed before starting the implementation of an ERP package.
Nov-04	[5(a)]	12	12.17 - 12.18	10	Write a detailed note on the expectations, fears and the ground realities that a corporate management faces during the post-implementation phase of ERP.
Nov-04	[7(b)]	12	12.8	5	Write short note : Business Process Re-engineering
May-05	[6(a)]	12	12.5-12.6	5	What are the characteristics and features of an ERP?
May-05	[6(b)]	12	12.19-12.20	5	List any five ERP Vendors and briefly describe the ERP packages offered by them
Nov-05	[4(b)]	12	12.6-12.7	10	What are the benefits achieved by implementing the ERP packages ?
Nov-05	[7(c)]	12	12.8	5	Business Engineering
May-06	[5(b)]	12	12.14-12.15	5	Explain the various criteria used for evaluation of the ERP packages.
Nov-06	[7(a)]	12	12.28-12.29	5	Enterprse Controlling
May-07	[2(b)]	12	12.18-12.19	10	How will you establish and implement Critical Success Factors(CSFs) and key Performance Indicators (KPIs) un an organisation for achieving the benefits of implementions of ERP?
Nov-07	[6(a)]	12	12.5-12.7	10	What is Enterprise Resources Planning? Briefly describe its benefits.
May-08	[4(a)]	12	12.5-12.6	5	Briefly explain the characteristics and features of an Enterprise Resource Planning.
Nov-08	[3(b)]	12	12.25-12.26	5	Discuss the functions and facilities provided by Treasury Cash Management module of an ERP package.
Nov-02	[1(b)]	13	13.29-13.34	10	What are the two major categories of exposures in the Communication subsystems including Internet and Intranet? What control mechanisms could be used to deal with them?
May-03	[7(e)]	13	13.34,13.35-13.36	5	Wtite short note : Personal Computer Controls
Nov-03	[1(d)]	13	13.23-13.26	10	What are the different types of securities required for the computer system? Explain briefly the different components of physical security of a computer installation.

May-04	[4(a)]	13	13.18-13.19	10	Discuss the activities dealing with system development controls in EDP setup.
May-04	[7(c)]	13	13.30-13.31	5	Write short note : Firewalls
Nov-04	[7(c)]	13	13.32 - 13.33	5	Write short note : Encryption
May-05	[4(c)]	13	13.913.11	5	Describe various access control methods used for safety of the database.
May-05	[5(a)]	13	13.26-13.28	10	What do you understand by disaster recovery plan? Discuss its various components.
Nov-05	[1(c)]	13		5	"No Company, big or small, can ignore the opportunity opened by the internet" What are the various methods by which internet can be accessed? What are the considerations for choosing the right alternatives?
Nov-05	[1(d)]	13		5	Mention any five security steps an internet user should take to protect from cyber crime and computer security threats
Nov-05	[5(b)]	13	13.8	5	Discuss various ways in which audit trail can be used to support security objectives?
May-06	[6(b)]	13	13.3-13.4	5	Describe the various security components available in secure Operating system.
May-06	[7](i)	13	13.30-13.31	5	Write Shot notes on any four of the following: (i) Firewalls
May-06	[7](iv)	13	13.20-13.22	5	Write Shot notes on any four of the following: (iv) Source program library control
Nov-06	[1(c)]	13	13.1-13.2	5	Differentiate between General and Application controls. Also mention the broad categories into which the first can be subdivided.
Nov-06	[5(c)]	13	13.29-13.30	5	What are the subversive threats? How do the intruders manipulate the message being transmitted?
May-07	[4(b)]	13	13.2-13.3	5	What are five control objectives of an Operating system?
Nov-07	[5(b)]	13	13.13-13.14	5	State and explain the four back up and recovery fearures necessary in a DBMS
May-08	[1(c)]	13	13-9-13.11	5	Briefly discuss any five database control features.
May-08	[6(c)]	13	13.21-13.23	5	Discuss how a controlled source program library environment can help to deter unauthorized changes to program.
May-08	[7(d)]	13	13.30-13.31	5	Write short note: Firewalls.
Nov-08	[6(a)]	13	13.26-13.28	10	What is 'Disaster Recovery Plan'? Discuss its various components.
Nov-08	[7(a)]	13	13.32-13.33	5	Write short note : Encryption techniques
Nov-03	[7(e)]	14	14.15,14.16	4	Write Short Note : Transaction logs
May-04	[4(b)]	14	14.2-14.3	5	What type of errors can corrupt a data code?
May-05	[7(a)]	14	14.16-14.17	5	Write short notes on: Transaction logs
Nov-05	[5(c)]	14	14.2	5	Explain the importance of sources documents and associated control techniques.
May-06	[5(a)]	14	14.6-14.12	10	What is the significance of input validation control? Describe briefly three different levels of input validation controls used in computerized information system
Nov-06	[1(b)]	14	14.7-14.9	5	Discuss some common types of field interrogation as a validation control procedures in a nEDP set up.
May-07	[1(a)]	14	14.16-14.17	5	Briefly describe the techniques used to preserve audit trails in a Computer Based Information system

Nov-08	[7(c)]	14	14.16-14.17	5	Write short note : Audit trail controls in Computer Based Information System (CBIS)
Nov-02	[6(a)]	15	15.15-15.16	10	What measures can be adopted to detect Computer Frauds?
May-03	[7(c)]	15	15.17	5	Wtite short note : Disc Imaging and analysis Technique
Nov-03	[5(c)]	15	15.3-15.4	10	Why should businesses take Computer Frauds seriously?
May-04	[4(c)]	15	15.4	5	What are the computer frauds commited through input?
May-04	[7(a)]	15	15.6-15.7	5	Write short note : Internet frauds
Nov-04	[6(a)]	15	15.7 - 15.9	10	Substantiate with reasons to the view that there is a steep rise in the Internet Computer fraud. Why many institutions are unable to contain it?
May-05	[1(c)]	15	15.4-15.7	5	Why is Computer fraud a serious threat to any business organisation?
May-05	[7(d)]	15	15.17	5	Write short notes on: Disc Imaging and Analysis Technique.
Nov-05	[5(a)]	15	15.13-15.15	10	What kind of controls can be incorporated in the system to make frauds difficult to perpetrate?
May-06	[1(d)]	15	15.9-15.11	5	Define the following computer Fraud and Abuse techniques. (i) Hacking (ii) Logic time bomb (iii) Piggy backing (iv) Spamming (v) Data didding
Nov-06	[4(c)]	15	15.4-15.5	5	How can computer fraud be commited using input in four different ways?
Nov-06	[7(d)]	15	15.6-15.7	5	Internet Frauds
May-07	[4(c)]	15	15.15-15.16	5	What steps can be taken to detect computer fraud?
Nov-07	[5(c)]	15	15.4-15.6	5	Briefly explain five categories of Computer frauds based on the data processing model.
May-08	[3(b)]	15	15.13-15.15	10	Briefly explain various kinds of controls that can be incorporated in the system to make frauds difficult to perpetrate.
May-08	[4(c)]	15	15.9-15.11	10	Define the following computer fraud and abuse technique: (i) War dialing (ii) Scavenging (iii) Cracking (iv) Internet terrorism (v) Masquerading.
Nov-08	[1(c)]	15		8	Recently you have received a report from your bank client that money from one account has been unauthorisedly transferred to another account by stealing the login information of a client through Internet. How will you stop the recurrence of such events?
Nov-02	[5(a)]	16	16.6,16.11	10	What is a Digital Signature? How is it used? What are the duties of certifying authorities in regard to its usage?
May-03	[1(a)]	16	16.3-16.6	10	Expalin briefly the scope of the Information Technology act, 2000 along with the relevant definitions that are used.
Nov-03	[7(c)]	16	16.6	4	Write Short Note : Digital Signature Certificate

May-04	[1(a)]	16	16.19	10	What are the powers of the Central Government to make rules, as given in Section 87, Chapter XIII of Information Technology act, 2000?
Nov-04	[1(b)(i)]	16	16.3	2	Define: (i) Affixing digital signature
Nov-04	[1(b)(ii)]	16	16.4	2	Define: (ii) Asymmetric crypto system
Nov-04	[1(b)(iii)]	16	16.4	2	Define: (iii) Computer network
Nov-04	[1(b)(iv)]	16	16.5	2	Define: (iv) Private and Public keys
Nov-04	[1(b)(v)]	16	16.5	2	Define: (v) Secure system
May-05	[1(b)]	16	16.2	5	State the objectives and scope of IT Act, 2000
Nov-05	[6(c)]	16	16.11	5	What are the duties of certifying authorities with respect to digital signature ?
May-06	[1(b)]	16	16.14-16.16	5	Describe the composition and powers of cyber regulatory appellate tribunal.
Nov-06	[5(a)]	16	16.16	10	Describe some of the powers of the cyber Apllelate Tribunal.
May-07	[5(b)]	16	16.21	5	Describe some of the powers of controller under section 89 to make regulations consistent with Information Technology Act, 2000.
Nov-07	[1(b)]	16	16.11	5	What are the duties of certifying authorities with respect to digital signature ?
Nov-07	[7(a)]	16	16.2	5	Objectives of Information Technology Act, 2000
May-08	[1(d)]	16	16.19-16.20	5	Discuss briefly the powers of Central Government under Section 87 to make rules in respect of Information Technology Act, 2000.
Nov-08	[1(b)]	16	16.14-16.16	4	Describe the composition and powers of cyber regulatory appellate tribunal.
Nov-08	[3(c)]	16	16.7-16.8	5	Discuss the main provisions provided in Information Technology Act, 2000 to facilitate E-governance.
Nov-02	[1(a)]	17	17.14-17.15	10	Describe the majour techniques of Concurrent audit of Information systems. Bring out the relevance of such audit.
May-03	[6(a)]	17	17.1-17.2	10	Discuss the various issues that are of primary concerns for an auditor involved in information systemaudit.
May-03	[7(b)]	17	17.15	5	Wtite short note : System Control audit Review File (SCaRF)
Nov-03	[1(a)]	17	17.1	2	What is the sole purpose of an Information System (IS) audit?
Nov-03	[1(b)]	17	17.4	2	What is the role of an IS auditor?
Nov-03	[1(c)]	17	17.3	6	While performing an IS audit, the auditor should make sure that various objectives are met. Briefly describe them.
May-04	[1(b)]	17	17.6-17.7	10	Briefly dicuss the frame work on which the auditor should work for the audit of Computer Security.
May-04	[7(b)]	17	17.4	5	Write short note : Integrated test facility
Nov-04	[1(a)]	17	17.14-17.15	10	"In On-line systems, conventional audit trail is difficult and almost impossible" Why? Explain the kind of audit techniques used in such system.

May-05	[1(a)]	17	17.13	10	Your client has recently switched over from manual accounting to computerised accounting. When you receive computerized accounts for the first quarter you find the following types of error:(i) Incomplete or unauthorized data input(ii) Errors in the files or database during updating(iii) Improper distribution or disclosure of output.You, as an information system auditor, suggest the suitable test of controls for audit of computer processing so that the above mentioned errors can be prevented.
Nov-05	[1(a)]	17	17.2-17.3	5	Discuss various factors that render manual audit method ineffective in IS audit.
Nov-05	[1(b)]	17	17.4	5	Briefly describe the various objectives to be met while performing an IS audit.
May-06	[1(a)]	17	17.18	5	A XYZ company receives orders from customers either by telephone, facsmile or electronic data interchange. A clerk then transcribes the order into one of the company's order from to be keyed into the order entry system. You being the information system auditor of the company, suggest various internal control procedures to be adopted to prevent inaccurate or unathorized source data entry?
Nov-06	[1(d)]	17		5	How does MIS auditing enhance the control process?
Nov-06	[7(b)]	17	17.14-17.15	5	Integrated Test Facility
May-07	[1(d)]	17	17.16-17.17	5	Various software packages serve as aids in analysis of program logic. Explian briefly.
May-07	[7(d)]	17	17.15	5	Snapshot tecnique
Nov-07	[1(a)]	17	17.4	5	While performing an IS audit, the auditor should ascertain that various objectives are properly met. Briefly describe them.
Nov-07	[7(b)]	17	17.3-17.4	5	Review areas of an IS Auditor
May-08	[1(a)]	17	17.2-17.3	5	Discuss various factors that render manual audit method ineffective in Information System audit.
Nov-08	[1(a)]	17	17.1-17.2	8	Discuss various issues that are of primary concern for an auditor involved in information System Audit.

<table>
<tr><td>Nov-08</td><td>[6(b)]</td><td>17</td><td></td><td>10</td><td>Persian Paints is a small but highly regarded paint manufacturing company. The company has a network in place linking many of its business operations. Though the firm believes that its security is adequate, the recent addition of a Web site has become an open invitation to hackers. Management requested a risk assessment. The risk assessment identified a number of potential exposures. These exposures, their associated probabilitie and average losses are summarized in the following table

<table>
<tr><td></td><td colspan="3">Persian Paints Risk Assessment</td></tr>
<tr><td></td><td>Exposure</td><td>Probability of Occurrence(%)</td><td>Annual Average Loss(Rs.)</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td>1</td><td>Virus attack</td><td>60</td><td>75,000.00</td></tr>
<tr><td>2</td><td>Data Loss</td><td>12</td><td>70,000.00</td></tr>
<tr><td>3</td><td>Embezzlement</td><td>3</td><td>30,000.00</td></tr>
<tr><td>4</td><td>User Errors</td><td>95</td><td>25,000.00</td></tr>
<tr><td>5</td><td>Threats from Hackers</td><td>95</td><td>90,000.00</td></tr>
<tr><td>6</td><td>Improper use by Employees</td><td>5</td><td>5,000.00</td></tr>
<tr><td>7</td><td>Power Failure</td><td>15</td><td>300,000.00</td></tr>
</table>
Using the above risk assessment data, calculate the expected annual loss for each exposure. Which control points have the greatest vulnerability and least vulnerability? Prepare a written report that summarized your findings and recommendations.</td></tr>
<tr><td>Nov-02</td><td>[5(b)]</td><td>18</td><td>18.7-18.10</td><td>10</td><td>What are the core principles of Information Security?</td></tr>
<tr><td>May-03</td><td>[1(b)]</td><td>18</td><td>18.20</td><td>10</td><td>Expalin the role played by an information security administrator.</td></tr>
<tr><td>Nov-03</td><td>[6(a)]</td><td>18</td><td>18.7-18.9</td><td>10</td><td>Briefly describe any five core principles of Information Security</td></tr>
<tr><td>May-04</td><td>[6(a)]</td><td>18</td><td>18.1-18.2</td><td>10</td><td>Explain in brief information security and its importance.</td></tr>
<tr><td>Nov-04</td><td>[6(b)]</td><td>18</td><td>18.17 - 18.19</td><td>10</td><td>Give an eg. of an Information Security Policy Statement.</td></tr>
<tr><td>May-05</td><td>[2(a)]</td><td>18</td><td>18.2-18.3</td><td>10</td><td>What is"Information Security"?State the core principles of Information Security.</td></tr>
<tr><td>May-06</td><td>[6(a)]</td><td>18</td><td>18.12-18.13</td><td>10</td><td>What do you mean by Information Security policy? Explain the silent features of the Information Security policy</td></tr>
<tr><td>Nov-06</td><td>[1(a)]</td><td>18</td><td></td><td>5</td><td>Why Computerized Information system are more vulnerable to many more kinds of threats than manual systems? Name some of the key areas where large amounts of data stored in eletronic form are most vulnerable.</td></tr>
<tr><td>Nov-06</td><td>[6(a)]</td><td>18</td><td></td><td>5</td><td>Nobody told you that your internet use in the office was being monitored. Now you have been warned you will be fired if you use the internet for recreational surfing again. What are your rights?</td></tr>
<tr><td>Nov-06</td><td>[6(b)]</td><td>18</td><td></td><td>7</td><td>Your employees are abusing their internet privileges, but you don't have an interent usage policy. What do you do?</td></tr>
</table>

Nov-06	[6(c)]	18		8	Employee Mr. X downloads adult material to his PC at work, and employee Miss Y sees it. Miss Y then proceeds to sue the company for sexual harassment. As the employer, are you liable?
Nov-06	[7(c)]	18	18.11	5	Restorative Information Protection
May-07	[1(b)]	18	18.12-18.13	5	Briefly outline the contents of Information Security policy.
May-07	[7(c)]	18	18.11-18.12	5	Holistic protection
Nov-07	[2(a)]	18	18.1-18.3	10	What is "Information Security"? Why is it important in any organization? Explain briefly
May-08	[6(a)]	18	18.12-18.17	5	Briefly explain the best approach to implement information security policy?
May-08	[6(d)]	18	18.20	5	Briefly explain the role of Information Security Administrator.
Nov-02	[7(b)]	19	19.1,19.3	5	Write short note : CaSE tools
May-03	[7(a)]	19	19.11	5	Write short note : Meta-CaSE Workbenches
Nov-03	[6(b)]	19	19.1-19.2,19.3-19.4	10	What are CaSE Tools? Describe in-depth the categories of CaSE tools with examples
May-04	[6(b)]	19	19.15	6	Explain the significance of ratio analysis generally carried out for financial analysis
May-04	[6(c)]	19	19.16	4	Explain briefly the profitability ratio
May-05	[6(c)]	19	19.7-19.8	10	What are called Work benches? Describe the various tools used in programming work bench.
Nov-05	[7(b)]	19	19.9	5	Analysis and design work bench
May-06	[5(c)]	19	19.12	5	Describe briefly five components of CASE work bench.
Nov-06	[5(b)]	19	19.4	5	What are the five different levels of integration on CASE tools?
May-07	[1(c)]	19	19.2-19.3	5	What are CASE Tools? Discuss briefly its three categories.
Nov-07	[3(a)]	19	19.10-19.11	10	Explain with the help of a diagram the various tools which are included in a testing workbench.
Nov-07	[7(c)]	19	19.6-19.7	5	Process Integration
May-08	[1(b)]	19	19.9-19.10	5	Briefly explain the components of an analysis and design work bench.
Nov-08	[7(b)]	19	19.10-19.11	5	Write short note : Testing work benches

Marks Allocation to Chapters

Marks		Year of Exam													
Group	Chapter No.	Nov-02	May-03	Nov-03	May-04	Nov-04	May-05	Nov-05	May-06	Nov-06	May-07	Nov-07	May-08	Nov-08	Grand Total
1	1		10		5			5	10		5	10	5	5	55
	2										5				5
	3	8	10	9	10	5	5		5	10			15	10	87
	4		15	11	8	15	10	10	15	10		5	5	10	114
	5	17		4		5	5	10	5		10	5	5	5	71
1 Total		25	35	24	23	25	20	25	35	20	20	20	30	30	332
2	6	8	10	8	12	20	5	5	5		5		5	5	88
2 Total		8	10	8	12	20	5	5	5		5		5	5	88
3	7	17	10	12	10	5	10	15	15	10	15	15	10	10	154
	8	10		4	10		15	10	5	5	10	5	5	5	84
	9		10	4	10	10	10	15	10	5	10	15	10	10	119
	10	5	10	8		10	5	5	5	5	15	10	5	5	88
3 Total		32	30	28	30	25	40	45	35	25	50	45	30	30	445
4	11	10	10	12		10			10	10	10	10	10	10	102
	12	10	10	10		15	10	15	5	5	10	10	5	5	110
4 Total		20	20	22		25	10	15	15	15	20	20	15	15	212
5	13	10	5	10	15	5	15	15	15	10	5	5	15	15	140
	14			4	5		5	5	10	5	5			5	44
	15	10	5	10	10	10	10	10	5	10	5	5	20	8	118
5 Total		20	10	24	30	15	30	30	30	25	15	10	35	28	302
6	16	10	10	4	10	10	5	5	5	10	5	10	5	9	98
6 Total		10	10	4	10	10	5	5	5	10	5	10	5	9	98
7	17	10	15	10	15	10	10	10	5	10	10	10	5	18	138
	18	10	10	10	10	10	10		10	30	10	10	10		130
	19	5	5	10	10		10	5	5	5	5	15	5	5	85
7 Total		25	30	30	35	20	30	15	20	45	25	35	20	23	353
Grand Total		140	145	140	140	140	140	140	145	140	140	140	140	140	1830