

PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

Question No. 1 is compulsory.

Answer any four questions from remaining six questions.

Question 1

- (a) Discuss various issues that are of primary concern for an auditor involved in Information System Audit.
- (b) Describe the composition and powers of Cyber Regulatory Appellate Tribunal.
- (c) 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?

(8 + 4 + 8 = 20 Marks)

Answer

- (a) Auditors involved in reviewing an information system should focus their concerns on the system's control aspects. They must look at the total system environment – not just the computerized segment. This requires their involvement from the time that a transaction is initiated until it is posted to the organization's general ledger. Specifically, auditors must ensure that provisions are made for:
 - An adequate audit trail so that transactions can be traced forward and backward through the system.
 - Controls over the accounting for all data entered into the system and controls to ensure the integrity of those transactions throughout the computerized segment of the system.
 - Handling exceptions and rejections from the computer system.
 - Testing to determine whether the system performs as stated.
 - Control over changes to the computer system to determine whether the proper authorization has been given.
 - Authorization procedures for system overrides.
 - Determining whether organization and government policies and procedures are adhered to in system implementation.
 - Training users in the operation of the system.
 - Developing detailed evaluation criteria, so that it is possible to determine whether the implemented system has met predetermined specifications.
 - Adequate controls between interconnected computer systems are put in place.

- Adequate security procedures to protect the user's data. Backup and recovery procedures for the operation of the system.
 - Technologies provided by different vendors are compatible and controlled.
 - Data bases are adequately designed and controlled to ensure that common definitions of data are used throughout the organization, that redundancy is eliminated or controlled, and that data existing in multiple data bases is updated concurrently.
- (b) The Cyber Regulations Appellate Tribunal shall consist of one person only (called, the presiding officer of the Tribunal) who shall be appointed by notification of the Central Government. The person must be qualified to be a judge of a High court or is or has been a member of the Indian Legal Service in the post in Grade I of that service for at least three years.

Section 58 provides for the procedure and power of the Cyber Appellate Tribunal. The Tribunal shall also have the powers of the civil court under the code of Civil Procedure 1908.

Some of the powers specified are in respect of the following matters:

- (a) Summoning and enforcing the attendance of any person and examining him on oath.
 - (b) Requiring production of documents and other electronic records.
 - (c) Receiving evidence of affidavits
 - (d) Reviewing its decisions
 - (e) Issuing commissions for examination of witness etc.
- (c) Most of the attacks on online banking used today are based on deceiving the user to steal login data and valid PINs. Two well known examples for those attacks are phishing and pharming. Cross-site scripting and key logger/Trojan horses can also be used to steal login information.

Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as user names, passwords and credit card details by masquerading as trust worthy entity in an electronic communication.

Pharming is hackers attack aiming to redirect websites traffic to another, bogus website. Pharming can be conducted either by changing the hosts file on a victims computer or by exploitation of a vulnerability in DNS server software.

Under such circumstances, all the customers must be informed about possible traps that they may fall into if they reveal their login and passwords. Continuous update and awareness should be created by the bank about various methods that are followed by

fraudsters. The company should have constant watch and vigil over such happenings and inform the customers immediately. To be more secure:

- (1) The Company should have a policy which states very clearly that no login information will be sought by the bank either in email, or over phone. This should be communicated to all customers.
- (2) There should be more than just two co-ordinates of login and password to make the transaction more secure. It can ask for additional details which are known only to the customer.
- (3) The company should educate the customers about the use of strong passwords and the benefits of changing the passwords.

Question 2

- (a) What is Payroll accounting? Describe in brief the inputs and master file, output and system flow diagram required for it.
- (b) 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. (10 + 10 = 20 Marks)

Answer

- (a) A payroll system is intended to basically produce pay slips and pay cheques for the employees every month. Preparing a payroll requires collecting employee work hours through their attendance cards, converting hours to gross earnings and computing deductions and net pay. Other activities to be performed as by products of payroll include accumulating summary data for general ledger reports, printing quarterly and year-end reporting statements and making labour distribution job costing or job performance measurements and reporting them. In addition to accounting activities, a payroll system also maintains record of sick leave, earned accruals and usage, and other details of the employees.

Inputs and Master File:

Master file: The payroll computer application uses a combination of current and year-to-date master computer file having records for the current period as well as for yearly reporting. The master file contains permanent as well as current data.

Information such as employee's rate of pay, accumulated earned leave, change in status code etc. are used as inputs to transform gross salary into net pay. The payroll master file may consist of following field:

Personnel Data:

Record code	Employee number	Employee name	Address	Phone number	Sex	Date of birth	Date started employment
-------------	-----------------	---------------	---------	--------------	-----	---------------	-------------------------

Payroll computation Data:

Job number	Department number	Type of cost code	Basic pay	Exempt status (exempt employees do not get extra pay for overtime)	Overtime rate
------------	-------------------	-------------------	-----------	--	---------------

Leave Data:

Earned leave accumulation rate	Sick leave accumulation rate	Accumulated Earned leave	Accumulated Sick leave	Earned leave used in this year	Sick leave used in this year
--------------------------------	------------------------------	--------------------------	------------------------	--------------------------------	------------------------------

Payment data for the payroll:

Current gross pay	Current dearness allowance	Current housing allowance	Special allowance	Current regular hours	Current overtime hours	Current provident fund	Current insurance premium	Current voluntary deductions	Current net pay	YTD gross pay	YTD income tax	YTD provident fund	YTD Insurance Premium	YTD Voluntary deductions	YTD hours
-------------------	----------------------------	---------------------------	-------------------	-----------------------	------------------------	------------------------	---------------------------	------------------------------	-----------------	---------------	----------------	--------------------	-----------------------	--------------------------	-----------

Transaction File:

Employee number	Regular hours	Overtime hours	Earned leave	Sick leave	Special deductions
-----------------	---------------	----------------	--------------	------------	--------------------

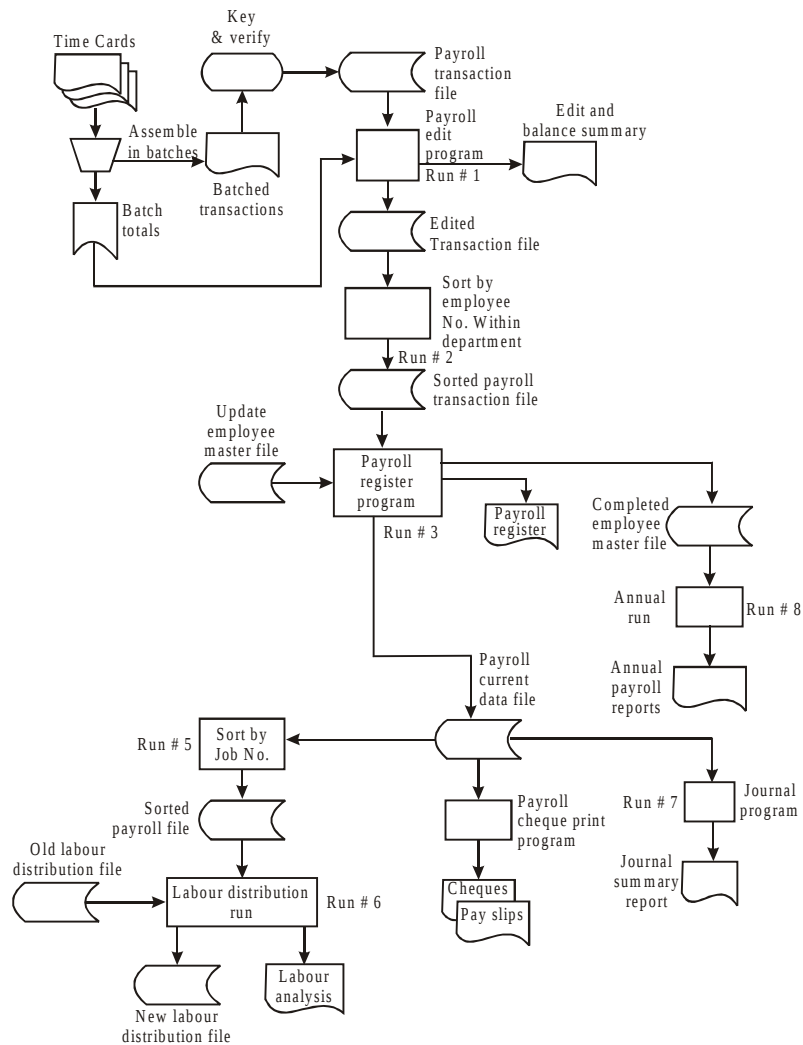
The permanent portion of the master file must be updated before current transactions are entered into the system. The accounting department also obtains data in new employees and recent changes to existing employees for updation of payroll master file. Inputs to the system consist of keyed data for time cards, batch control information and the employee master file updated by the preliminary master file update.

Outputs: The payroll accounting system produces following Outputs:

- Cheques, pay slips of employees
- Labour analysis – Job No. wise and trade wise
- Payroll Budget Report – Amount v/s Description head (i.e. salary, income tax etc.)
- Payroll Journal summary – quarterly, annual basis.

The system flow chart is given below:

System flow diagram

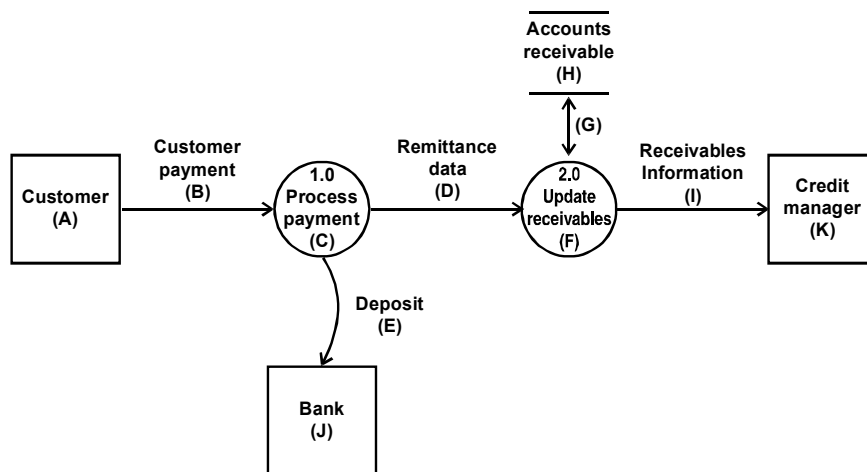


Payroll Accounting

- (b) System development tools are used to help end users and systems analysts to improve current information systems and to develop new ones. Their main purposes are
- To conceptualize, clarify, document and communicate the activities and resources involved in the organisation and its information systems.
 - To analyze present business operations, management decision making and information processing activities of the organisation.
 - To propose and design new or improved information systems to solve business problems or pursue business opportunities that have been identified.

The major tools used for system development can be divided under four categories based on the systems features documentation as discussed below:

1. **System Components and Flows:** These tools help the system analysts to document the data flow among the major resources and activities of an information system. They show the flow of data as they are processed by the hardware devices and manual activities. A Data Flow Diagram (DFD) uses a few simple symbols to illustrate the flow of data among entities (such as people or organisations etc.), processing activities and data storage elements. A system component matrix provides a matrix framework to document the resources used, the activities performed and the information produced by the information system. A DFD is drawn below:



2. **User Interface:** A friendly interface between end users and the computer system is a major consideration. Layout forms and screens are used to construct the formats and contents of input/output media and methods. Data flow diagrams analyze the flow of dialogue through an Information system. They document the flows among different display screens generated by alternative end user responses to menus and prompts.

Figure below illustrates a layout screen for the design of a customer order form.

CUSTOMER ORDER FORM				
DATE MM/DD/YY				
ORDER NUMBER	9999			
CUSTOMER NAME	XXXXXXXXXXXXXXXXXXXXXX			
CATALOG NUMBER	AVAILABLE	LOCATION	COST	DELMODE
XXXXXXXXXXXXXX	X	XXXXXXX	999.99	XXXX
XXXXXXXXXXXXXX	X	XXXXXXX	999.99	XXXX

3. Data attributes and relationships: The data resources in information system are defined, catalogued and designed by this category of tools. A data – dictionary catalogs the description of attributes (characteristics) of all data elements and their relationships to each other as well as to external systems. Entity-relationship diagrams are used to document the number and type of relationship among entities in a system. File layout forms document type, size and names of the data elements in a system. Grid charts help in identifying the use of each type of data element in input/output or storage media of a system. An example of a data dictionary is drawn below:

Name of data field	File in which stored	Source document	Size in bytes	Type
Inventory quantity on hand	Inventory master file	Form number ABC 123	4	Numeric

← Data dictionary

4. Detailed system process: These tools are used to help the programmer to develop detailed procedures and processes required in the design of a computer program. Decision trees and decision tables are drawn in a network or tabular form to document the complex conditional logic involved to select from alternatives. Structure charts document the purpose, structure and hierarchical relationships of the modules in a program. A decision table is represented below:

		Granting Credit Facility	R1	R2	R3	
Part 1	C1	Credit limit Okay	Y	N	N	Part 3
	C2	Pay experience Favourable	-	Y	N	
Part 2	A1	Allow Credit Facility	X	X		
	A2	Reject Order			X	Part 4

Question 3

- (a) What is Financial decision making? Which Financial decisions are made with the help of Financial information system?
- (b) Discuss the functions and facilities provided by Treasury Cash Management module of an ERP package.
- (c) Discuss the main provisions provided in Information Technology Act, 2000 to facilitate E-governance. (10 + 5 + 5 = 20 Marks)

Answer

- (a) Financial Decision Making: It deals with procurement of funds and their effective utilization in the business. There are two important aspects of financial decision making – first relates to decisions regarding procurement of funds and second to decisions regarding effective utilization of funds in the business.

Procurement of funds is a complex problem since there are number of sources from where the funds may be raised for long-term such as equity, debentures, bonds etc. or on short-term such as banks, suppliers, credit etc. These sources have different characteristics in terms of risk, control and cost.

Effective utilization of funds implies deployment of funds in several long term and short term assets, properly and profitably. The funds are procured at a certain cost with a certain level of risk. If they are not utilized in a manner as to generate higher income over their cost, they will cause losses to business. Thus, each decision should be properly analysed while investing in fixed assets.

Financial Decisions by Financial Information Systems are as under:

- (i) Estimation of requirements of funds: A careful estimation of funds and the timing or period of their need is to be made. This can be done by forecasting all physical activities of the firm and translating them into monetary units.
- (ii) Capital Structure Decision: Decisions are to be taken to select an optimum mix of different sources of capital structure, and various options available for procuring funds. Ratio between debt and equity, long term and short term funds etc needs to be decided such that the company is able to procure funds at minimum costs.
- (iii) Capital Budgeting Decisions: Funds procured from different sources are required to be invested in different assets. Capital budgeting helps to determine feasibility of investment in long term assets as per financial objectives.
- (iv) Profit Planning: Financial decisions concerning profits and dividends are to be taken such that adequate surpluses exist in future for growth and distribution of dividends.
- (v) Tax Management: Tax planning is aimed at reducing cash outflow by way of taxes so that the same may be effectively utilized for the benefit of business. Tax planning

must make full advantage of exemptions, deductions, concessions, rebates, allowances and other reliefs.

- (vi) Working Capital Management: It deals with investment of long term funds into current assets. Effective financing of current assets can be: achieved for day-to-day running of the organisation by working capital management.
 - (vii) Current Asset Management: Policy decisions are taken regarding various items of current assets. Credit policy determines the amount of sundry debtors at any point of time. Inventory policy is to be determined jointly between finance and production department.
- (b) Treasury Cash Management: Treasury Cash Management component allows the analysis of financial transactions for a given period. It identifies and records future developments for the purpose of financial budgeting.

In Treasury Cash Management, the company's payment transactions are grouped into cash holdings, cash inflows and cash outflows. Cash Management module provides:

- (i) Information on the sources and uses of funds to secure liquidity to meet payment obligations when they become due.
 - (ii) Monitors and controls incoming and outgoing payments flows.
 - (iii) Supplies data required for managing short term market investment and borrowings.
 - (iv) Enables to know current cash position, short term cash management and medium and long term financial budgeting.
 - (v) Enables analysis of liquidity.
 - (vi) Helps in cash management decisions.
 - (vii) In bank accounting, it helps in electronic banking and control functions for managing and monitoring of bank accounts.
 - (viii) The liquidity forecast function integrates anticipated payment flows from financial accounting, purchasing and sales to create liquidity outlook from medium to long term.
 - (ix) Covers foreign currency holdings and foreign currency items.
- (c) E-Governance: Sections 6, 7 and 8 of chapter III are the main sections for provisions related to E-governance provided in IT Act, 2000 to facilitate e-governance.

Section 6 lays down the foundation of electronic Governance. It provides that the filling of any form, application or other documents; creation, retention or preservation of records, issue or grant of any license or permit; receipt or payment in Government offices and its agencies may be done by 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.

Section 7 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 under the following conditions:

- (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 the origin, destinations, dates and time of despatch or receipt of such electronic record to be dispatched or received.

This section does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received. Moreover this section does not apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

Section 8 provides for the publication of rules, regulations, order, bye-law and notifications in the official Gazette in an electronic form. It provides that where any law requires the publication of any rule regulation, order, bye law, notification or any other matter in the Official Gazette, both in the printed as well as in the electronic form, the date of publication shall be the date of publication of the Official Gazette which was first published in any form.

Question 4

- (a) 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.
- (b) What control techniques can be utilized for increasing security in a client-server model?
- (c) What are the characteristics of good coding scheme for data input?

(10 + 5 + 5 = 20 Marks)

Answer

- (a) The following points may be considered while selecting a computer system:
 - Today all computer systems available in the market have good hardware, competent software and roughly similar facilities. Due to rapid advances in computer technology, more recent computers are better in performance and the lower in cost. Hence as far as possible, the latest possible technology should be acquired in general.
 - Commercial data processing involves mainly reading-in-data, printing data, storing and retrieving information from media. For commercial work computer performance is affected by the speed and capabilities of input/output and storage peripherals in contrast to scientific, engineering and operations problems which require good computational facilities, hence the efficiency of a computer system in handling such

problems will depend on the main storage available. A comparison along these lines may be made.

- The software supplied by the manufacturer may make a significant difference if it contains a package of special applicability to the jobs envisaged. The selection of computer can also be made on software considerations. While all manufacturers supply general software packages for documentation and linear programming etc, a few manufacturers also offer packages specially designed for a particular industry such as Accounting applications in banking and insurance. Obviously, a manufacturer who has a package for users special needs will enjoy a significant advantage.
- Modern computers are marketed as series of compatible, increasingly powerful and interchangeable peripherals. After some period, work expands beyond to fit in the existing computer needing higher capacity machine. Also, in case of breakdown, compatibility allows a wider range of machines to be used as back-up. Thus, the choice of a computer really becomes the choice of the model within the series, based on the long-range plan of expansion. But dependence on vendor/server is preferable to reprogramming which can be prohibitively expensive or time consuming. The selection of the computer configuration and a plan for its gradual expansion, as a properly considered model can save a great deal of money. The computer systems must be forward and backward compatible.
- Outside assistance in computer selection can be had from computer manufacturers, independent consultants specializing in computers, or management consulting firms. The distinction between vendor selection and machine selection is essentially a matter of business judgment. Once, however, the vendor is selected, he can be counted upon to provide useful guidance for machine also.

Point scoring Table for 'Ready to use' software:-

Software Evaluation Criteria	Possible points	Vendor A	Vendor B	Vendor C
Does the software's meet the mandatory specifications?	10	7	9	6
Will program modifications, if any, be minimal to meet company needs?	10	8	9	7
Does the software contain adequate controls?	10	9	9	8
Is the performance (speed, accuracy, reliability etc.) adequate?	10	7	9	6
Are other users satisfied with the software?	8	6	7	5
Is the software user-friendly?	10	7	8	6
Can the software be demonstrated and	9	8	8	7

test-driven?				
Does the software have an adequate warranty?	8	6	7	6
Is the software flexible and easily maintained?	8	5	7	6
Is online inquiry of files and records possible?	10	8	9	7
Will the vendor keep the software up to date?	10	8	8	7
Total	123	94	106	85

It may be noted that the data shown above are indicative only.

(b) Client/Server Security:

Client/server technology utilise distributed techniques, thus there is an increased risk of unauthorised access to data and modification. To increase the security; following techniques can be utilised:

- Disabling the floppy disk drives, ports, and use of Diskless workstations to control unauthorized access and thus securing data and applications.
- Unauthorised users can be prevented from overriding login scripts and access by securing automatic boot or start up batch file.
- Monitoring of the client using detective control technique can help network security and aid later investigations.
- Data encryption techniques can be used to protect data from unauthorized access.
- Authentication systems can be provided for a client so that they can enter into system only by entering login name and password.
- Use of smart cards i.e. intelligent hand held devices and encryption techniques can be used to decipher random 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.
- Applications controls may be used and users should be limited to access only those functions in the system those are required to perform their duties.

(c) Codes are used to express data/information to reduce input, control errors and to speed up the entire process. A code is a brief number, title or symbol used instead of lengthy or ambiguous description. With code, fewer details are necessary in computer input but it may result in loss of information.

Some of the desired characteristics of good coding schemes are enumerated below:

- (i) **Individuality:** The code must identify each object in a set uniquely and precisely. Use of same code number for several types of objects in a set causes great confusions. Further, the code should be universally used over the entire organization.
- (ii) **Space:** A code number must be much compact than description.
- (iii) **Convenience:** The formats of code numbers should facilitate their use by people i.e. it should be short, simple and consist of digits and / or upper case alphabets. It is better to avoid the use of special symbols like hyphens, oblique, dot etc.
- (iv) **Expandability:** As far as possible future growth in number of objects in a set should be provided for i.e. longer number of digit/number than necessary at present may be adopted as the code length. Related items must use fundamentally similar numbers.
- (v) **Suggestiveness:** The logic of the coding scheme should be readily understandable. Also the letter or number should be suggestive of the item characteristics. But this should not be carried too far in lengthening the code since it would defeat the purpose of brevity.
- (vi) **Permanence:** Changing circumstances should not invalidate the coding scheme or in other words invalidation in the future should not be considered.

Question 5

- (a) What is Executive Information System (EIS)? How does EIS differ from Traditional Information Systems?
- (b) Define and differentiate between 'Scheduled maintenance' and 'Rescue maintenance' along with their respective benefits.
- (c) 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? (5 + 5 + 10 = 20 Marks)

Answer

- (a) An Executive Information System (EIS) is referred to as an executive support system that is designed to meet the special needs of top-level managers. It is a tool that provides direct on-line access to relevant information in a useful and navigable format, which is timely, accurate and actionable about aspects of a business that are of particular interest to the senior manager.

EIS differs from traditional information systems in the following manner:

- (i) These are specifically tailored to meet executive's information needs and particularly easy to use (typically mouse or touch screen driven). EIS require large amounts of storage capacity and processing power both 'within the system and the network.

- (ii) These have ability to access data about specific issues and problems as well as aggregate reports. Also these provide extensive on-line analysis tools including trend analysis and exception reporting.
 - (iii) EIS present information in summary format, with facility to 'drill down' to other levels of information. They have ability to manipulate data to project 'what if' outcomes and have modeling tools to work with internal and external information.
 - (iv) EIS tend to be externally-focused, strategically-based systems using both internal and external data, whereas other computer systems mainly concentrate on internal control aspects of the organization.
- (b) Most information systems need some modifications after development. This need arises from time to time, due to failures to anticipate all requirements during system design and/or due to changed organisational needs. The changing needs impact most information systems and thus regular systems maintenance involves adding new data elements, modifying reports, adding new reports, changing calculations etc.

Such maintenance can be categorised in the following two ways:

- (1) Scheduled Maintenance is undertaken for tasks which can be anticipated and can be planned for in advance. An information system may remain in an operational and maintenance mode for several years. The system should be evaluated periodically to ensure that it is operating properly and is still workable for the organisation.
 - (2) Rescue maintenance refers to previously undetected malfunctions or such sudden changes that were not anticipated but require immediate solution. A system that is properly developed and tested should have few occasions of rescue maintenance. Rescue maintenance is unplanned and generally puts system stand still.
- (c) Evaluation of MIS:

An effective MIS should be capable of meeting the information requirements of its executives in present and future as well. This capability can be maintained by evaluating the MIS and taking appropriate timely action. The evaluation of MIS should take into account the following points:

- (1) Examining whether enough flexibility exists in the system, to cope with any expected or unexpected information requirement in future.
- (2) Ascertaining the views of users and the designers about the capabilities and deficiencies of the system.
- (3) Guiding the appropriate authority about the steps to be taken to maintain effectiveness of MIS.

The following factors should be considered for designing an effective MIS:

- (1) Management Oriented: The development of Management Information system should start from assessment of management needs and overall business objectives. Such system does not only take care of the information

requirements of the top management but it also caters to the information needs of the middle and operating levels of management.

- (2) **Management Directed:** As MIS is oriented towards the information needs of the management; it is essential that management should direct the development efforts of such systems on an on-going basis. Management should devote sufficient time not only at the stage of conceptualization and designing, but also for the regular reviews of its effectiveness. In short, management should play the key role in setting the system specifications as well as subsequent trade-off occurring in system development.
- (3) **Integrated:** All functional and operational information sub-systems should be integrated into one entity. Such Information system has the potential of generating meaningful and comprehensive information to management.
- (4) **Common Data flows:** For such integrated information system, data is captured only once and as close to its original generating source as possible. This eliminates duplication in data collection, documents and procedures. It also simplifies operations and produces an efficient and effective information system. However, the duplication cannot be avoided to some extent in order to ensure effective information system.
- (5) **Meticulous Planning:** It takes 3 to 5 years, sometimes even longer period, to get the MIS system established firmly in an organization. Therefore, there should be meticulous planning in designing and development of MIS system. It should be designed considering the future objectives and information needs of the organization. The system obsolescence should be avoided before it becomes operational.
- (6) **Sub Systems approach:** Although MIS is considered to be a single entity; it is broken into various sub systems so that it can be implemented one at a time by developing the systems in phases. This ensures meaningful and effective implementation of information systems.
- (7) **Common Database:** The common database holds all functional systems together, consolidates and also integrates data of all functional systems. The access to this database is allowed to the users of sub systems on need-to-know and need-to-do basis. It eliminates duplication in data storage, updating and protection as well as optimizes the cost of data storage and management.
- (8) **Computerized:** MIS can also be established using a manual system, but use of computers increases the effectiveness of the system. In fact, it equips the information system to handle variety of applications by catering quickly to their information requirements.

While designing an MIS, it should also be considered that computerization has following effects on management Information Systems:

- (1) High speed of data processing and retrieval.

- (2) Expanded scope of use of Information system.
- (3) Wide scope analysis.
- (4) Increased complexity of system design and operations.
- (5) Integrated functioning of various information sub-systems.
- (6) Enhanced effectiveness of Information Systems.
- (7) Comprehensive Information.

Question 6

- (a) What is 'Disaster Recovery Plan'? Discuss its various components.
- (b) 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
2. Data Loss	12	70,000
3. Embezzlement	3	30,000
4. User Errors	95	25,000
5. Threats from Hackers	95	90,000
6. Improper use by Employees	5	5,000
7. Power Failure	15	3,00,000

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 summarises your findings and recommendations.

(10 + 10 = 20 Marks)

Answer

- (a) 'Disaster Recovery' implies contingency measures that organisation adopt at key computing sites to recover from or to prevent momentary bad events or disasters such as fire, flood, earthquake etc. or a violent takeover, willful or accidental destruction of equipments or other acts of such nature.

Disaster Recovery Plan (DRP): With careful planning, the impact of disaster can be absorbed and the organisation can recover. DRP assures a set time after disaster occurrence to minimise losses to the organisation and restore normalcy.

The general components of the plan would be as follows:

- (1) Emergency Plan: It provides for actions to be taken as soon a disaster occurs which are stated below:
 - It identifies the personnel to be notified immediately i.e. fire service, police, management, insurance company etc.
 - It provides guidelines on guides equipment shutdown, termination of power supply, removal of storage files and removable disks if any.
 - It sets out evacuation procedures like sounding the alarm bell, activating fire extinguishers, evacuation of personnel etc.
 - It provides return procedures as soon the primary facility gets ready for operation such as back up files to be brought from the off-site, deleting data from disk drives at third party's site, relocation of proper versions of backup files etc.
- (2) Recovery Plan: This part of DRP sets steps for restoration of full capabilities. A recovery committee is constituted to set priorities for recovery operations to undertake following:
 - (i) An inventory of the hardware, application systems, system software, documentation etc. must be taken.
 - (ii) Criticality of application systems to the organisation and the importance of loss are evaluated. An indication of the efforts and cost involved in restoring the various application systems is made.
 - (iii) An application system hierarchy is decided to accept a degraded mode of operation.
 - (iv) Selection of a disaster recovery site such as a reciprocal agreement with another organisation having compatible hardware and software could be made, considering system availability and data security. Hiring a service bureau or a fully operational backup site could be other alternatives.
 - (v) A formal backup agreement with another company may be done to cover the periodical exchange of information between two sites regarding changes to hardware/ software, the time and duration of system availability, modalities of testing plan etc.
- (3) Backup Plan: Despite recovery procedures, systems are still vulnerable to disasters. A safeguard could also be destroyed be it hardware or software. Thus stand-by hardware, keeping copies of important programs, data files, operating systems and test programs etc. help get back into operation quickly. These backups

must be kept at separate places which are not susceptible to the same hazard as the originals.

- (4) Test Plan: This plan is required to look after the testing of the Disaster Recovery Plan (DRP) i.e. to identify deficiencies in the emergency, backup or recovery plan. It defines procedures for testing the plan like –

- Paper walk-through: It involves critical personnel in the plan's execution reasoning out what might happen in the event of different disasters.
- Localised Tests: It simulates system crash on different aspects of the plan.
- Full operational test: It is nearer to disaster conditions. Paper walk-through and localised tests should have been conducted before completely shutting down operations to simulate disasters.

- (b) Persian Points Company has recently added a website and this has opened up invitation to hackers and the management is in the process of assessing its risk management. Various risk assessment factors are identified. The annual average losses and the associated problems are provided. We can calculate the expected monetary losses for each of the potential exposures.

	Exposure	Expected Monetary Loss		Rs.
1.	Virus Attack	$0.60 \times 75,000$	=	45,000
2.	Data loss	$0.12 \times 70,000$	=	8,400
3.	Embezzlement	$0.03 \times 30,000$	=	900
4.	User Errors	$0.95 \times 25,000$	=	23,750
5.	Threats from Hackers	$0.95 \times 90,000$	=	85,500
6.	Improper use by Employees	$0.05 \times 5,000$	=	250
7.	Power Failure	$0.15 \times 3,00,000$	=	45,000

Amongst all the expected monetary losses listed in the above table, Item No. 5 results in the highest expected loss. Hence, "threats from hackers" has the highest vulnerability. Item No. 6, "improper use by employees" has the least vulnerability since it results in the least expected loss.

A careful analysis of the last column in the above table would show that the top management should exercise control by having a careful watch on the following factors in the following order of priority as listed below:

- (i) Threats from Hackers (Item 5)
- (ii) Virus Attack (Item 1) and power failure (Item 7).
- (iii) User errors (Item 4)
- (iv) Data Loss (Item 2)

- (v) Embezzlement (Item 3)
- (vi) Improper use by employees (Item 6).

Question 7

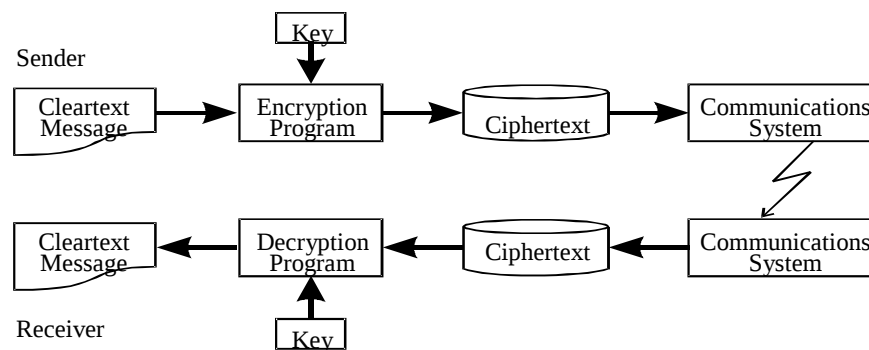
Write short notes on the following:

- (a) Encryption techniques
- (b) Testing work benches
- (c) Audit trail controls in Computer Based Information System (CBIS)
- (d) Expert systems. (4 × 5 = 20 Marks)

Answer

- (a) **Encryption Technique:** It is the conversion of data into secret code for storage in databases and transmission over networks. The sender uses an encryption algorithm to convert the original message called clear text into a coded equivalent called cipher text. At the receiving end, cipher text is decoded back into clear text. The encryption algorithm uses a key, which is a binary number ranging typically from 56 to 128 bits in length. The more bits in the key, the stronger is the encryption method. Two general approaches used are private key and public key encryption.

Private Key Encryption: Data encryption standard (DES) uses a single key known to both the sender and the receiver of the message. To encode a message, the sender provides the encryption algorithm with the key, to produce a cipher text message. The encoded message is transmitted to the receiver, which decodes the message with a decryption program that uses the same key employed by the sender. Figure given below illustrates this technique.



In DES approach, a perpetrator may discover the key and intercept and decipher the message. The more individuals who know the key, the greater is the probability of it falling into wrong hands.

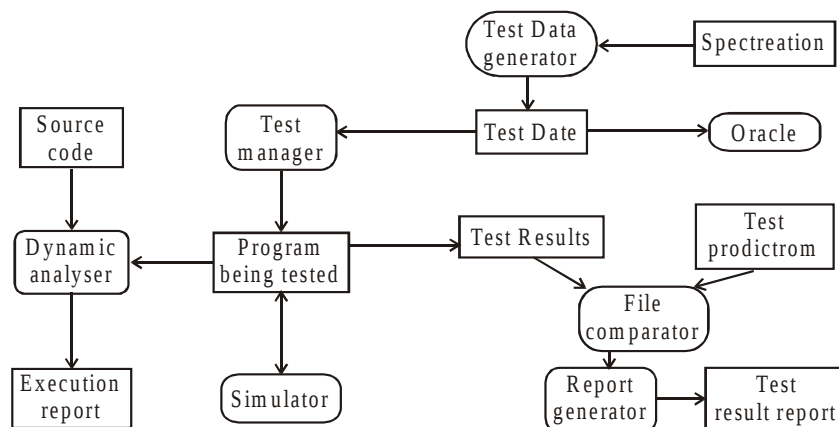
Public Key Encryption: It uses separate keys for encoding messages and for decoding them. Each recipient has a private key that is kept secret and a public key to encrypt the message. The receiver then uses his or her private key to decrypt the message. Users never need to share their private keys to decrypt messages, thus reducing the likelihood that they fall into the hands of a criminal.

- (b) Testing Workbenches: These 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. It keeps track of test data, expected 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 the expected results.
- (d) File compactor: Compares the results 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.

A typical testing workbench layout is shown in the figure.



- (c) **Audit Trail Controls in CBIS:** Every transaction must be traceable through each stage of processing from its economic source to its presentation in financial statements. In CBIS environment, the audit trail can become fragmented and difficult to follow. The following techniques can be used to preserve audit trails in a CBIS:
 - (a) **Transactions Logs:** Every successful transaction should be recorded on a transaction log, which serves as a journal. Thus the transaction log becomes permanent record of validated transactions etc. those that have changed account balances. Unsuccessful transactions are placed in error file. The consolidation of transaction log and error files accounts for all transactions.
 - (b) **Transaction Listing:** The system should produce a hard-copy transaction listing of all successful transactions which may be reconciled by users.
 - (c) **Log and Listing of Automatic Transactions:** Some transactions are triggered internally by the system. All internally generated transactions must be placed in transaction log to maintain an audit trail. The responsible end user should receive detailed listing.
 - (d) **Unique Transaction Identifiers:** Each transaction processed by the system must be uniquely identified with a transaction number among thousands of records. In real-time systems, each validated transaction is assigned a unique number by the system.
 - (e) **Error Listing:** A listing of all error records should go to the appropriate user to support error correction and resubmission.
- (d) **Expert Systems:** An expert system is software that attempts to reproduce the performance of one or more human experts, and is a traditional application of artificial intelligence.

Expert Systems are designed to replace the need for a human expert. They are particularly important where expertise is scarce and therefore expensive. This is not 'number-crunching' software, but software that expresses knowledge in terms of facts and rules. This knowledge will be in a specific area, and therefore expert systems are not general, as are most decision support systems which can be applied to most scenarios, an expert system for oil drilling is not of much use in solving company taxation problems.

While there may have been a progression from transaction – processing systems, through management information systems, to decision-support and executive information systems, expert systems have arisen largely from academic research into artificial intelligence. 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 or expert systems shells which can make the process quicker and easier. It has been suggested that expert systems would be of greater use in the tactical and strategic level. This has been the case in banking, where expert systems scrutinize applications for loans, and lower level staff accepts the system's decision. This has replaced the somewhat subjective decision-making of most senior managers.