

PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

Question No. 1 is compulsory.

Answer any four questions from remaining six questions.

Question 1

- (a) Explain the three tests that can be used to detect unauthorized or erroneous program changes.
- (b) State the objectives on which an Information system auditor should focus.
- (c) What is a computer fraud and what types of activities does it include?
- (d) Briefly explain the four common cycles of business activity along with listing some of the application systems for each cycle. (5 x 4 = 20 Marks)

Answer

- (a) To test for unauthorized or erroneous program changes, auditors can use a source code comparison program. After auditors thoroughly test a newly developed program, they keep a copy of its source code. At any subsequent time, the auditor may use the comparison program to compare the current version of the program with the original source code. If no changes have been authorized, these two versions should be identical. Therefore any unauthorized differences should result in an investigation. If the difference represents an authorized change, the auditor can refer to the program change specifications to ensure that the changes were authorized and correctly incorporated.

The reprocessing technique also uses a verified copy of the source code. On a surprise basis, the auditor uses the program to reprocess data and compare that output with the company's data. Discrepancies in the two sets of output are investigated to ascertain their cause.

Parallel simulation is similar to reprocessing except that the auditor writes a program instead of saving a verified copy of the source code. The auditor's result is compared with the company's and any differences are investigated. Parallel simulation can be used to test a program during the implementation process.

- (b) An information system auditor should focus on the following objectives:
 - (i) Security provisions to protect computer equipments, programs and data from unauthorized access, modification or destruction.
 - (ii) Program development and acquisition is done in accordance with managements' general and specific authorization.
 - (iii) Program modifications have the authorization and approval of the management.
 - (iv) Processing of transaction files, reports, and other computer records is accurate and complete.

PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

- (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.
- (c) Computer frauds have been defined as any illegal act for which knowledge of computer technology is essential for its perpetration, investigation or prosecution. It might be generally thought that computer fraud means no more than “using a computer to commit fraud”. This is far too narrow a definition in view of the many ways that businesses can face the risk of loss as a result of the use or misuse of a computer. A more extensive definition of computer fraud could be given below:

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

Most specifically, computer frauds include the following:

- Unauthorised theft, use, access, modification, copying and destruction of software or data
- Theft of money by altering computer records or the theft of computer time
- Theft or destruction of computer hardware
- Use or the conspiracy to use computer resources to commit an offence
- Intend to illegally obtain information or tangible property through the use of computer

Using the computer, fraud perpetrators are able to steal more, in much less time and with much less efforts. For example, they can steal millions of rupees in less than a second. Perpetrators can commit a fraud and leave little or no evidence. Therefore, computer fraud is often much more difficult to detect than other types of frauds.

Most frauds have as their object the financial benefit of the fraudster and consequent financial loss to the victim. An equally serious threat to business also arises from activity which is not fraudulent in the traditional sense but which, nonetheless, has the potential to cause damage to the reputation of a business.

- (d) The four common cycles along with application systems are discussed below :
 - (i) Revenue Cycle: It comprises of events related to the distribution of goods and services to other entities and the collection of related payments. Application systems may be – customer order entry, billing, accounts receivable etc.
 - (ii) Expenditure Cycle: It comprises of events related to the acquisition of goods and services from other entities and the settlement of related obligations. Application systems may be – purchasing, accounts payable and payroll etc.

FINAL EXAMINATION : JUNE, 2009

- (iii) Production Cycle: It comprises of events related to the transformation of goods, and services. Application systems may be – production control and reporting product costing etc.
- (iv) Finance Cycle: It comprises of events related to the acquisition and management of Capital Funds, including cash. Application system can be – Cash management, debt management etc.

Question 2

- (a) State and briefly explain the major categories and the items included therein to estimate the information system costs.
- (b) Why organisations fail to achieve their system development objectives?
- (c) What is an Audit risk? Distinguish between errors and irregularities. Which do you think concern auditors the most? (8+8+4 = 20 Marks)

Answer

- (a) Information system cost can be sub-divided into (i) Development, (ii) Operational and (iii) Intangible cost.

Development costs for a computer based information system include costs of the system development process. It may include following items:

- Salaries of system analysts and computer programmers who design and develop the system.
- Costs of converting and preparing data files and preparing system manual and other supporting documents.
- Costs of preparing new or expanding computer facilities.
- Costs of testing and documenting the system, training employees and other startup costs.

Items included in operating costs are as stated below:

- Hardware/Software rental or depreciation charges.
- Salaries of computer operators and other computer personnel.
- Salaries of system analysts and computer programmer who perform the system maintenance function.
- Cost of input data preparation and control.
- Cost of data processing supplies.
- Cost of maintaining physical facilities.
- Overhead charges of the business firm.

PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

Intangible costs are those costs which cannot be easily measured. For example.

- Development of a new system may disrupt the activities of an organization and cause a loss of employee productivity or morale.
- Customer sales and goodwill may be lost by errors made during the installation of new system.

Such costs are difficult to measure in rupees, but are directly related to introduction and operation of the information system.

(b) There are many reasons why organizations fail to achieve their systems development objectives. Some of them are briefly discussed below:

1. Lack of senior management support for and involvement in information system development: Developers and users of information systems will watch senior management to determine which systems development projects are important and will act accordingly by shifting their effort away from any project not receiving management attention. In addition management can see that adequate resources, as well as budgetary control over the use of those resources, are dedicated to the project.
2. Shifting user needs: User requirements for information technology are constantly changing, as these changes accelerate, there will be more requests for systems development and more development projects. When these changes occur during a development process, the development team may be faced with the challenge of developing systems whose very purposes have changed since the development process began.
3. Development of strategic system: Because strategic decision making is unstructured, the requirements, specifications and objectives for such development projects are difficult to define; and determining “successful” development will be elusive.
4. New technologies: When an organization tries to create a competitive advantage by applying advanced information technology, it generally finds that attaining systems development objectives is more difficult because personnel are not as familiar with the technology.
5. Lack of standard project management and systems development methodologies: Some organizations do not formalize their project management and systems development methodologies, thereby making it very difficult to consistently complete projects on time or within budget.
6. Over-worked or under-trained development staff: Estimates of the systems development work facing development staffs range up to 4 years. In addition to being overworked, system developers often lack sufficient education background. Furthermore, many companies do little to help their development personnel stay technically updated; in these organizations, a training plan and training budget do not exist.

FINAL EXAMINATION : JUNE, 2009

7. Resistance to change: People have a natural tendency to resist change, and information systems development projects signal changes – often radical – in the workplace. Business process reengineering is often the catalyst for the systems development project. When personnel perceive that the project will result in personnel cutbacks, threatened personnel may block the progress of the project and the project may fail. Personnel cutbacks often result when reengineering projects are really attempts at “downsizing”.
 8. Lack of user participation: Users must participate in the development effort to define their requirements, feel ownership for project success, and work to resolve development problems. User participation also helps reduce user resistance to change.
 9. Inadequate testing and user training: New systems must be tested before installation to determine that they will operate correctly. Users must be trained to effectively utilize the new system.
- (c) An audit risk is the probability that the auditor will render an unqualified (clean) opinion on financial statements that are, in fact, materially misstated.

An error represents an unintentional misstatement of the financial statement. Errors are unintentional mistakes. It may be material or immaterial. Irregularities are intentional misrepresentation to perpetrate a fraud or to mislead the users of financial statements which can be material. Material misstatements may be caused by errors or irregularities or both.

While any auditor's objective is to minimize the audit risk by performing tests of control and substantive tests, the main concern of an auditor is to detect irregularities.

Question 3

- (a) List and describe the contents of a system manual
- (b) The Software industry continues to undergo constant changes; users need to be aware of recent trends and issues to be effective in their business and personal life. Explain.
- (c) Draw schematic chart of general form of business applications. (8+8+4 = 20 Marks)

Answer

- (a) The contents of a system manual include the following:
 - (i) General description of the existing system.
 - (ii) Flow of the existing system.
 - (iii) Outputs of the existing system – The documents produced by the existing system are listed and briefly described, including distribution of copies.
 - (iv) General description of the new system – its purposes and functions and major differences from the existing system are stated together with a brief justification for the change.

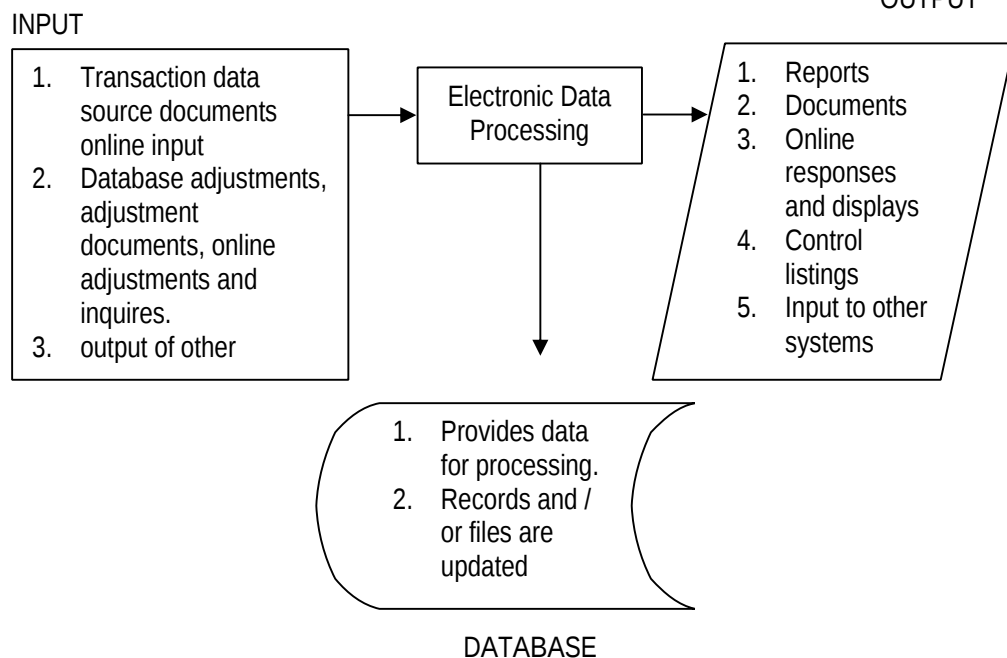
PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

- (v) Flow of the new system – this shows the flow of the system from and to the computer operation and the flow within the computer department.
 - (vi) Output layouts
 - (vii) Output distribution – the distribution of the new output document is indicated and the number of copies, routing and purpose in each department shown. The output distribution is summarized to show what each department will receive as a part of the proposed system.
 - (viii) Input layouts – the inputs to the new system are described and complete layouts of the input documents and input disks or tapes provided.
 - (ix) Input responsibilities – the source of each input document is indicated as also the user department responsible for each item on the input documents.
 - (x) Macro-logic – the overall logic of the internal flows to be briefly described.
 - (xi) Files to be maintained – the specifications will contain a listing of the tapes, disks, or other permanent records, and the items of information to be included in each file.
 - (xii) List of programs – a list of the programs to be written shall be a part of the systems specifications.
 - (xiii) Timing estimates – a summary of approximate computer timing is provided by the system analyst.
 - (xiv) Controls – this shall include type of controls and the methods in which it will be operated.
 - (xv) Audit trail – audit trail for all financial information and the methods by which errors and defects will be prevented or eliminated.
 - (xvi) Glossary of terms used.
- (b) It is true that software industry is undergoing constant changes; hence the users need to be aware of recent trends and issues. Software bugs, software licensing and copyrighting, open-source software, shareware and freeware, multi-organisational software development, software upgrades and global software support are all important software issues and trends which are briefly explained below:
- A software bug is a defect in a computer program that keeps it from performing in the manner intended. Software bugs are common, even in key pieces of business software.
 - Open-source software is software that is freely available to anyone in a form that can be easily modified. Open-source software development and maintenance is a collaborative process with developers around the world using the internet to keep in close contact via e-mail and to download and submit new software. Shareware and freeware can reduce the cost of software, but sometimes they might not be as powerful as commercial software. Also, their source code formally cannot be modified.

FINAL EXAMINATION : JUNE, 2009

- Multi-organisation software development is the process of extending software development beyond a single organisation by finding others who share the same business problem and involving them in a common development effort.
- Software upgrades are an important source of increased revenue for software manufactures and can provide useful new functionality and improved quality for software users.
- Global software support is an important consideration for large, global companies putting together standardised, company-wide system. A common solution is outsourcing global support to one or more third-party software distributors.

(c) The schematic chart of general form of business application is given below:



Question 4

- (a) State the inputs, processing and the outputs of a "Share Accounting System".
- (b) State the steps to be taken to reduce the threat from destructive programs.
- (c) List the main threats from hacking (8+8+4 = 20 Marks)

Answer

(a) Main inputs in a share accounting system are:

- Shareholding data from a fresh issue this is usually supplied by the issue agency on electronic media.
- Share transfer request

PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

- Split request
- Consolidation request
- Request for bank mandate
- Request for tax exemption forms
- Request for duplicate certificates
- Request for duplicate dividend warranties
- Change in shareholder's address

Processing of a share accounting system involves the following:

- Updating shareholders' master file
- Recording the transfer of shares
- Handling splitting, consolidation, and duplicate requests and printing new certificates.
- Calculation of dividend and income tax to be deducted

Main outputs of the share accounting system are:

- Transferred share certificates
- New share certificates in case of consolidation, splitting and duplicates.
- Dividend warrants and counterfoils.
- Statements of tax-deductions.

- (b) Destructive computer program refers to a computer program that performs a destructive function or produces a destructive result. A program performs a destructive function if it degrades performance of the affected computer, associated peripherals or a computer program; disables the computer, associated peripherals or a computer program; or destroys or alters computer programs or data. Threats from destructive programs can be substantially reduced through a combination of technology controls and administrative procedures. The following steps can be taken to reduce the threat from destructive programs:
- (i) Purchase software only from reputed vendors in original, and only product that are in their original factory - sealed covers should be accepted.
 - (ii) All software should be scanned for viruses and subsequently loaded and/or distributed only after the product is shown to be free of viruses. This includes all initial loads as well as any upgrades or changes applied to the software.
 - (iii) Conduct user training program to raise user awareness about preventive strategy to deal with destructive program.

FINAL EXAMINATION : JUNE, 2009

- (iv) Install all new applications on a stand – alone computer and implement on main server or LAN only after testing them thoroughly with anti-virus software.
 - (v) Keep servers, workstations and other network devices up to date with security patches and service packs. If possible enable automatic updates on all systems.
 - (vi) Routinely make back copies of key files. There is always a chance that the programs may catch something damaging or, the hard drive may crash. In such situation, backup can be used to restore the program.
 - (vii) Use anti-virus software with current virus signatures. Configure the anti-virus software to monitor files in real-time if possible, and configure automatic daily update of virus signatures if possible.
 - (viii) Keep track of software upgrades, patch and service packs. Update the software on regular basis.
- (c) Hacking is a process of breaking into computers, usually by gaining access without legal authorization to a computer or computer network. The main threats from hacking are:
- (i) Removal or loss of information
 - (ii) Destruction of system integrity
 - (iii) Interference with Web pages
 - (iv) Transmission of virus by email
 - (v) Interception of email, electronic payments and data packets over Internet.
 - (vi) Subverting computer security without authorization or using technology (usually a computer or the Internet) for vandalism (malicious destruction), credit card fraud, identity theft, intellectual property theft, or other types of crime.
 - (vii) Interception of data packets, which can be used to capture passwords and other data in transit over the network.
 - (viii) The hackers can carry out spoofing attack, which involves one program, system, or website successfully masquerading as another by falsifying data and thereby being treated as a trusted system by a user or another program. The purpose of this is usually to fool programs, systems, or users into revealing confidential information, such as user names and passwords, to the attacker (also known as Phishing).
 - (ix) The hackers can also take control of your computer remotely and access confidential information, launch denial of service attacks and scan ports among other destructive things.

Question 5

- (a) Consider the problem of long delays between receipts of orders and delivery in a company. Give the six steps in the system approach to find the solution for the above problem.

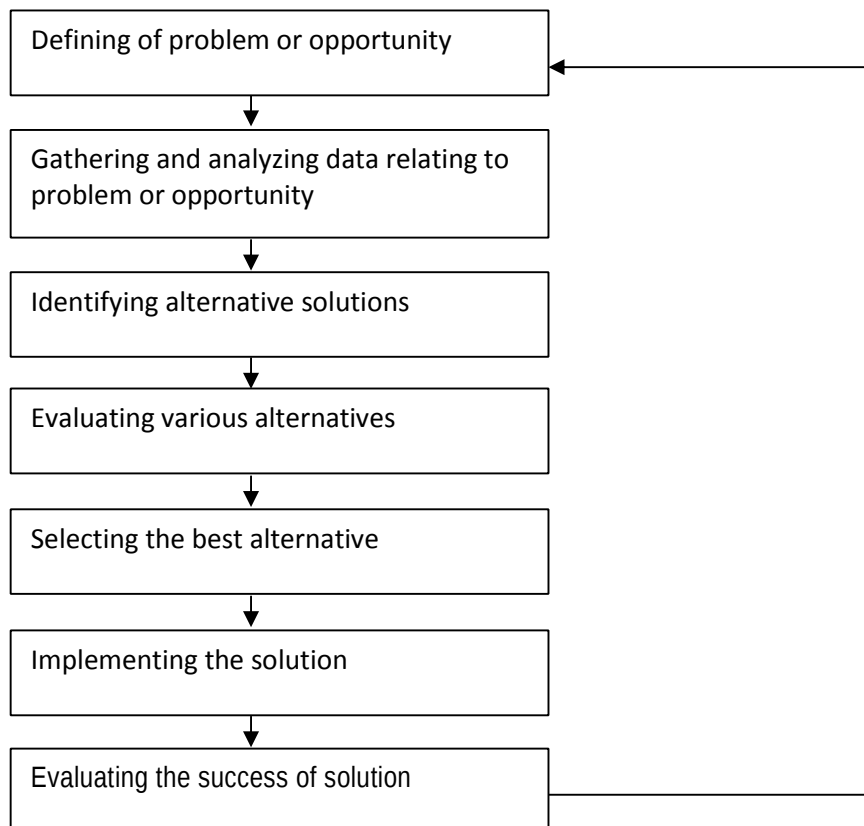
PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

- (b) Define top level management. What is the main responsibility of top management? Give the information requirement at top level for making decision.
- (c) What is a programmed and a non-programmed decision? Distinguish the difference between the two through an example. (8+8+4 = 20 Marks)

Answer

- (a) To seek solution for the problem of long delays between receipts of orders and delivery in a company by applying systems approach, we would make use of the six steps as shown in the diagram given below. Each of these steps with reference to the given problem is discussed below:

- (i) Defining the problem: The problem involved here is of inordinate delay between the receipts of orders and their delivery. This problem affects the vendor in many ways, e.g., a bad reputation, loss of customers, reduction in profitability and even stoppage of due payments.
- (ii) Gathering and analyzing data concerning the problem: The problem of delay in meeting orders, in this case, say arises due to the following reasons:
- Excessive orders in the hand of vendors
 - Shortage of power (fall in production due to shortage of power)



FINAL EXAMINATION : JUNE, 2009

- (iii) Identification of alternative solutions: To overcome the stated problem by system approach, the following two solutions may be considered:
- Refusal of orders, in case the total size of orders exceeds the plant capacity of one shift.
 - To run the plant in double shift, to meet the commitment in time. Any shortfall in power supply may be met by installing a generator.
- (iv) Evaluation of alternative solution: Out of the two identified solutions mentioned under the preceding step, the second solution say accounts for an overall increase in profitability of the concern after offsetting additional cost for the generator produced power. It also helps in retaining customers and growth of the concern.
- (v) Selection of the best alternative: Under this step, management examines the alternatives more closely and puts its stamp on the best possible alternative. In this case say the second alternative is finally chosen.
- (vi) Implementation of the solution: The implementation of the solution requires the necessary policy changes. Besides this, the resources required to run the plant in double shift and installation of generators are also to be arranged. Finally, appropriate procedures are developed to exercise smooth production and timely supply to customers and the concerned officers are accordingly instructed.
- (b) Top level management: It is defined as a set of management positions which are concerned with the overall task designing, directing and managing the organisation in an integrated manner.

The main responsibilities of the top management are in the direction of determining the overall goals and objectives of the business. It deals mainly with long term plans, policy matters and broad objectives of the company. Also, it establishes a budget frame work under which the various departments will operate.

The information requirements at top level for decision making are:

- Top management needs information on the trends in the external environment and on the functioning of the internal organizational sub-system.
- Apart from historical information, top management requires ongoing or current information also which is generated through forecasts of the future.

Thus, mostly the information utilized by top management is futuristic and external in nature. Much of the information so generated for strategic planning purpose tends to be incomplete and not fully reliable. It may not be available on time. For control purposes, top management receives summary and 'exception reports' from the middle management.

PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

The information requirement at top level for making decisions can be categorised into two parts:

- (a) External
 - Competitive activities
 - Customer preferences, style, changes
 - Economic trends
 - Technological changes, legal rulings.
- (b) Internal
 - Historical sales, costs
 - Profit, cash flow, divisional income, sales, expenses.
 - Financial ratios, interests, credit outstanding, long term debt, delinquent accounts.
 - Projects' progress reports and cost updates
- (c) Programmed decisions refer to decisions made on problems and situations by reference to a pre-determined set of precedents, procedures, techniques and rules. These are well structured in advance and pre-decided rule or procedure is applied to arrive at the decision. Non-programmed decisions are those that deal with unusual, non repetitive or exceptional situations. Decisions are taken by application of managerial intelligence, experience, judgment and vision.

The example of programmed decision is: ordering more inventories when the level drops to 100 units or fewer in a retail shop. The example of non-programmed decision is determining the best training for a new employee joining the organization.

Question 6

- (a) List the items of information provided by cash management of Treasury module of SAP.
- (b) Discuss the factors to be considered for valuation of a vendor's proposal.
- (c) List the fears that are expected to arise among employees of an organization during implementation of ERP (8+8+4 = 20 Marks)

Answer

- (a) The list of items of information provided by cash management of Treasury module is as follows:
 - (i) Information on 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 for short-term money market investment and borrowings.

FINAL EXAMINATION : JUNE, 2009

- (iv) Enables to know current cash position, short-term cash management, medium and long term financial budgeting.
 - (v) Enable 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.
- (b) The following factors need to be considered for valuation of a vendor's proposal:
- (i) Performance capability of each proposed system in relation to its cost: There are different ways to measure the performance. Indicator should be chosen according to the requirements of the organisation. There are many measures of performance such as speed of processing, response time, number of users supported, system configuration etc. One way to examine the operating efficiency of a particular system is to use a benchmark test.
 - (ii) Costs and benefits of each system: A cost-benefit analysis of each proposed system should be carried out. Lease-buy decision should also be considered, and also the depreciation schedule.
 - (iii) Maintainability of each proposed system: The ease with which a proposed computer system can be modified. Costs of maintaining are high therefore this factor should be seriously considered. The maintenance cost of large systems like ERP packages is very high, sometimes manifolds of the initial purchase cost. Considerable emphasis should be given on this dimension and must be incorporated in validation process.
 - (iv) Compatibility of each proposed system with the existing system: It is the ability to implement and interface the new system with existing computer resources and software. Compatibility can also involve the operating system, existing application software, or procedural aspects.
 - (v) Vendor support: It includes (i) training the employees, (ii) help in implementing and testing, the new system, (iii) assistance in maintaining the new system, (iv) back-up system.
- (c) Some of the fears which are expected to arise among employees of an organisation during ERP implementation are:
- Job redundancy – loss of job
 - Loss of importance – as information is no longer an individual's prerogative.
 - Change in job profile.

PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

- An organisational fear of loss of proper control and authorization.
- Increased stress caused by greater transparency.
- Individual fear of loss of authority.

Question 7

- (a) List and explain the Software packages that are helpful in analysis of program logic.
- (b) State the entities to which the Information Technology Act, 2000 does not apply.
- (c) State the methods through which awareness of employees towards security policy can be increased.
- (d) Discuss the advantages of pre-written application Software Packages. (5 x 4 = 20 Marks)

Answer

- (a) The following software packages help in program logic analysis:
 - (i) Automatic Flow Charting Program: It interprets program source code and generates a corresponding program flow chart.
 - (ii) Automated Decision Table Program: It generates a decision table representing the program logic.
 - (iii) Scanning Routines: It searches a program for occurrence of specified variable names or other character combinations.
 - (iv) Mapping Programs: It identifies unexecuted program code. This software can also uncover some unscrupulous programs.
 - (v) Program Tracing: It sequentially prints all application program steps, executed during a program run. Program tracing helps auditors in detecting unauthorized instructions incorrect, logic paths, and unexecuted program code.
- (b) The Information Technology Act, 2000 does not apply to the followings:
 - (i) A negotiable instrument as defined in section 13 of Negotiable Instruments Act, 1981;
 - (ii) A Power of Attorney as defined in section 1A Powers of Attorney Act, 1882;
 - (iii) A trust as defined in section 3 of Indian Trust Act, 1882;
 - (iv) A will as defined in section (h) of section (2) of Indian Succession Act, 1925 including any other testamentary disposition by whatever name called.
 - (v) Any contract for sale or conveyance – immovable property or any interest in such property.
 - (vi) Any such class of documents or transactions as may be notified in the Official Gazette by Central Government.

FINAL EXAMINATION : JUNE, 2009

- (c) Following are some of the ways through which employees' awareness towards security policy can be increased:
- Pasting the security policies on the notice board or in areas which are more frequently visited by employees.
 - Training to all the staff.
 - Non-disclosure statements signed by the employees.
 - Company newsletter.
 - Visible enforcement of security rules.
 - Periodic audits.
 - Conduct fake security incidents to improve security procedures.
- (d) The advantages of using pre-written application packages are as follows:
- (i) Rapid implementation: Readily available for implementation after purchase, whereas in-house developed software may take months.
 - (ii) Low risk: Since such packages are available in finished form, so the purchaser knows what is expected for what price, whereas in-house development entails uncertainty regarding time & cost.
 - (iii) Quality: The firms engaged in application packages development, have the expertise and the experience in the area, hence can provide better software.
 - (iv) Cost: An application package generally cost less as compared against developing in-house. The developing firms have the advantage of realizing the cost by selling at lower cost to large number of users.