

PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

Question No. 1 is compulsory. Answer **any four** questions from the remaining six questions.

All questions carry equal marks.

Question 1

- (a) *"In On-line systems, conventional audit trail is difficult and almost impossible." Why? Explain the kind of audit techniques used in such system.* (10 marks)
- (b) *Define the following important terms in the light of the Section 2 of the I.T. Act, 2000 :*
- (i) *Affixing digital signature*
 - (ii) *Asymmetric crypto system*
 - (iii) *Computer network*
 - (iv) *Private and Public keys*
 - (v) *Secure system.* (10 marks)

Answer

- (a) Historically, auditors have placed substantial reliance in evidence-collection work on the paper trail that documents the sequence of events that have occurred within an information system. Paper based audit trails have been progressively disappearing as online computer-based systems have replaced manual systems and as source documents have given a way to screen based inputs and outputs. In a batch processing system, one can still expect to find a visible trail of "run-to-run " controls, which can be reconciled to the original input batch totals. In such systems, it is unusual to find any significant loss of audit trails regarding the control totals. In online systems, however, data are stored in device-oriented rather than human-oriented form. Moreover, data files belonging to more than one application may be updated simultaneously by each individual transaction. In such systems, traditional run-to-run controls do not exist and the potential for loss of audit trail is significant.

In a batch processing systems, the test data is prepared by an auditor for audit purposes and the results are obtained from the program under execution and copy of relevant files. The results are compared with the predetermined correct outputs. Any discrepancies indicating processing errors or control deficiencies etc. are thoroughly investigated. In on-line systems, such kind of audit trail is not desirable since millions of transactions can be processed in a short time. In such cases, evidence gathered after data processing is insufficient for audit purposes. In addition, since many on-line systems process transactions continuously, it is difficult or impossible to stop the system in order to perform audit tests. Hence, the auditor needs to identify problems that can occur in an information system on a more timely basis. For this reason, a set of audit techniques has been developed to collect evidence at the same time as an application system undertakes processing of its production data.

Following are some of the audit techniques, which are being used for on-line systems :

- (A) **Concurrent Audit Techniques:** These techniques can be used to continually monitor the system and collect audit evidence while live data are processed during regular operating hours. As the name suggests, this type of audit technique uses embedded audit modules, which are segments of program codes that perform audit functions. They also report test results to the auditors and store the evidence collected for the auditor's review. These techniques are often time consuming and difficult to use, but are less so, if incorporated when programs are developed.

There are five such techniques, which auditors commonly use. These are :

- (i) **Integrated Test Facility (ITF) :** In this technique, a small set of fictitious records is placed in the master file. Processing test transactions to update these dummy records will not affect the actual records. Actual and fictitious records are concurrently processed together, without the knowledge of employees. Auditor compares the output of dummy records with expected results and its controls to verify the correctness of the system.
- (ii) **Snapshot Technique :** This technique examines the way transactions are processed. Selected transactions are marked with special code that triggers the snapshot processes. Audit modules in the program record these transactions and their master file records before and after processing. Snapshot data are recorded in a special file and reviewed by the auditor to verify that all processing steps have been properly executed.
- (iii) **SCARF :** System Control Audit Review File uses embedded audit modules to continuously monitor transaction activities and collect data on transactions with special audit significance. The data is recorded in a SCARF file, which may have been exceptional transactions. Periodically the auditor receives a print out of the SCARF file, examines the information to identify any questionable transactions, and performs any necessary follow up investigation.
- (iv) **Audit Hooks :** These are audit routines that flag suspicious transactions. When audit hooks are employed, auditors can be informed of questionable transactions as soon as they occur. This approach, known as "real-time notification", displays a message on the auditor's terminal.
- (v) **CIS :** Continuous and intermittent simulation embeds an audit module in a DBMS. This module examines all transactions that update the DBMS using criterion similar to those of SCARF. If a transaction has special audit significance, the module independently processes the data, records the results and compares them with those obtained by the DBMS. Discrepancies are noted and details are investigated.

- (B) **Analysis of program logic:** If a serious natured unauthorized code is found, the auditor goes for detailed analysis of the program logic. This is a difficult task and

the auditor must be well versed with the programming language. These days following software packages serve as aids in this analysis.

- Automated flowcharting programs
- Automated decision table programs.
- Scanning Routine.
- Mapping Programs.
- Program tracing.

(b) The definition of important terms according to Section 2 of the Information Technology Act, 2000 is as under:

- (i) **“Affixing digital signature”** with its grammatical variation and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature.
- (ii) **“Asymmetric crypto system”** means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.
- (iii) **“Computer network”** means the interconnection of one or more computers through –
 - (a) the use of satellite, microwave, terrestrial line or other communication media; and
 - (b) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained.
- (iv) **“Private and public keys”** refer to a key pair used in an asymmetric crypto system. Private key means the key used to create a digital signature whereas public key is used to verify the same and is listed in the Digital Signature Certificate.
- (v) **“Secure system”** means computer hardware, software and procedures that
 - are reasonably secure from unauthorized access and misuse;
 - provide a reasonable level of reliability and correct operation;
 - are reasonably suited to performing the intended functions; and
 - adhere to generally accepted security procedures.

Question 2

- (a) *What are the production information requirements of a GM (Production and Operations Management) with regard to production planning and control ?* (10 marks)
- (b) *What are the variables that the top management should consider during negotiations with the labour unions?* (5 marks)

- (c) *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. (5 marks)*

Answer

- (a) The production planning and control system involves two main procedures: the specification of materials and operations requirements and production scheduling. The information requirements of a GM for the materials and operations phase of any organisation are as stated below:

- (i) Firm's policy with regard to production of various products.
- (ii) Sales order, sales forecast, stock position, order backlog.
- (iii) Available labour force with their capabilities
- (iv) Standards of labour time, material, machine time and overhead cost etc.
- (v) Schedule of meeting the sales orders, region-wise, territory-wise etc.
- (vi) Quality norms for materials to be used and for the finished products.
- (vii) Break-up of the jobs and their resource requirements.

Planning the specific time at which product items should be manufactured is known as production scheduling. The information is required by the production-scheduling department so as to meet the following objectives:

- (i) to determine the stages of production in sequential and rational order;
- (ii) to minimise the idle time on the part of the operators and equipments;
- (iii) to assess the extent of need for subcontracting to outside parties;
- (iv) to ensure that completion dates and target dates of completing the production plans are met fully; and
- (v) to study alternative methods to performing the activities so that time taken to perform can be further reduced.

- (b) Many types of labour today are unionized. Unionized organisations usually have strict regulations regarding such items as pay scales, hiring and firing, promotions and working conditions. Management has the choice of trade – offs on the following variables during negotiations with the labour unions

- (i) Wage raise
- (ii) Paid holidays
- (iii) Contribution to employees, insurance and pension plan
- (iv) Overtime premiums.

Cost accountants/payroll accountants would be in the best position to make various estimates for the cost implication of trade off.

- (c) It is true that to a large extent, executives rely much more on their own intuition, gut feelings and past experience rather than on sophisticated analytical skills. The type of decisions that the executives must make is broad. Often, executives make these decisions based on a vision they have regarding what it will take to make their companies successful. The intuitive character of executive decision-making is reflected strongly in the types of information found most useful to executives.

Five characteristics of the types of information used in executive decision-making are discussed below:

- (i) **Lack of structure:** Many of the decisions made by executives are relatively unstructured. For instance, what general direction should the company take? Or what type of advertising campaign will best promote the new product line? These types of decisions are not so clear-cut as deciding how to debut a computer program or how to deal with an overdue account balance. Also, it is not always obvious which data are required or how to weigh available data when reaching at a decision.
- (ii) **High degree of uncertainty:** Executives work in a decision space that is often characterized by lack of precedent. For example, when the Arab oil embargo hit in the mid-1970s, no such previous event could be referenced for advice. Executives also work in a decision space where results are not scientifically predictable from actions. If prices are lowered, for instance, product demand will not automatically increase.
- (iii) **Future orientation:** Strategic-planning decisions are made in order to shape future events. As conditions change, organisations must also change. It is the executive's responsibility to make sure that the organisation keeps pointed toward the future. Some key questions about the future include: "How will future technologies affect what the company is currently doing? Where will the economy move next, and how might that affect consumer buying patterns? As one can see, the answers to all of these questions about the future external environment are vital.
- (iv) **Informal source:** Executives rely heavily on informal source for key information. For example, lunch with a colleague in another firm might reveal some important competitor strategies. Some other important information sources of information are meetings, tours around the company's facilities to chat with employees, brainstorming with a trusted colleague or two, and social events. Informal sources such as television might also feature news of momentous concerns to the executives.
- (v) **Low level of detail:** Most important executive decisions are made by observing broad trends. This requires the executive to be more aware of the large overviews than the tiny items. Even so, many executives insist that the answers to some questions can only be found by mucking through details.

Question 3

- (a) *Define a 2-tier and a 3-tier architecture.* (2 marks)
- (b) *What are the control techniques to be checked to ensure security for client/server technology?* (8 marks)
- (c) *Describe four categories of risks that are to be considered during the transition from the mainframe (or PC) to client/server.* (10 marks)

Answer

- (a) **2-tier and 3-tier architecture:** 2-tier refers to fat clients and 3-tier refers to fat servers in a client/server architecture. Fat client and fat-server serve as vivid descriptions of the type of client/server systems in place. In a fat-client system, more of the processing takes place on the client, like with a file server or database server. Fat-servers place more emphasis on the server and try to minimise the processing done by the clients. Examples of fat-servers are transaction, Groupware, and the web servers.
- (b) To increase the security for client / server technology, an IS auditor should ensure that the following control techniques are in place:
- ♣ Access to data and application is secured by disabling the floppy disk drive.
 - ♣ Diskless workstation prevents unauthorized access.
 - ♣ Unauthorized users may be prevented from overriding login scripts and access by securing automatic boot or startup batch files.
 - ♣ Network monitoring can be done to know about the client so that it will be helpful for later investigation, if it is monitored properly. Various network-monitoring devices are used for this purpose. Since this is a detective control technique, the network administrator must continuously monitor the activities and maintain the devices, otherwise these tools become useless.
 - ♣ Data encryption techniques are used to protect data from unauthorized access.
 - ♣ Authentication systems can be provided to a client, so that they can enter into system, only by entering login name and password.
 - ♣ Smart cards can be used. It uses intelligent hand-held devices and encryption techniques 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.
 - ♣ Application controls may be used and users will be limited to access only those functions in the system that are required to perform their duties.

(c) There are risks involved in the transition from mainframe (or PC) to client/server. These risks can be classified into four categories as discussed below:

- (i) **Technological Risk:** The technological risk is quite simple- Will the new system work? The short-term aspect of this question is -will it literally work? But more important aspect of the risk is that in the long run the system may grow obsolete. That it will become obsolete is probably inevitable thus the question becomes-how soon will it become obsolete. To resolve this issue, the firm and the IT consultant/division should understand system standards and market trends and use them in their decision making processes while deciding what system to incorporate into their organisation.
- (ii) **Operational Risks:** These risks parallel the technological risks in both the short and long run. Respectively, they are: will the organisation achieve the performance it needs from the new technology and will the software that it chooses be able to grow or adapt to the changing needs of the business. Once again sound planning and keeping an eye to the future are the only remedies for these risks.
- (iii) **Economic Risks:** In the short run, firms are susceptible to hidden costs associated with the initial implementation of the new client/server system. Cost will rise in the short term since one needs to maintain the old system (mainframe) and the new client server architecture development. In the long run, the concern centres around the support costs of the new system.
- (iv) **Political Risks:** Finally, political (people) risks involved in this transition are addressed. Here, the short-term question is-will end users and management be satisfied? The answer to this is definitely not if the system is difficult to use or is plagued with problems.

The long run question concerns costs, unless the mainframe is completely replaced, the total cost of transaction processing for the organisation as a whole goes up and this creates political problems.

Question 4

- (a) *List the various sources of acquiring the software.* (5 marks)
- (b) *Discuss four most compelling advantages of using a pre-written application package* . (5 marks)
- (c) *"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.* (10 marks)

Answer

- (a) Once the computer hardware is decided, the question of software acquisition becomes important for the management. Some system software is supplied by the manufacturer, which may make a significant difference if it contains a package of special applicability to the job envisaged. Different sources for software acquisition are explained below:

- (i) At the time of selection of hardware, it should be identified which manufacturer supplies general/particular software.

It has been observed that all manufacturers supply general software packages for LP, PERT etc. and packages for such commercial applications as inventory control and production planning etc. A few manufacturers also offer packages specially designed for a particular industry such as airline reservation, banking and insurance.

- (ii) After deciding user outputs and input designs, the system developer may decide to create the software in-house i.e. a 'make decision'.
 - (iii) At this stage, the decision may be taken to acquire the software from the vendor. This decision is often called the 'buy decision'. In market, several pre-packaged application software in many business functions, including accounting, general ledger etc. are available. Therefore, they could be directly purchased, and personnels be trained to start the work immediately.
 - (iv) Computer manufacturers, large and small software houses and computer retail stores are some of the sources from where software packages can be purchased.
 - (v) There are user groups or association of users of a particular computer system, which are the sources of packaged software. These softwares are developed by one member organisation and made available to other members.
- (b) **Advantages of Pre-written Application Packages:** The four most compelling advantages of using pre-written application packages are summarized below:
- (i) **Rapid implementation:** Application packages are readily available to implement after they are purchased. In contrast, software developed in-house may take months or even years until it is ready for implementation.
 - (ii) **Low risk:** Since the application package is available in the finished form, the organisation knows what it is going to get for the price it has paid. With in-house developed software, the long development time breeds uncertainty with regard to both the quality of the final product and its final cost.
 - (iii) **Quality:** The firms engaged in application package developments are typically specialist in their products' niche area. Generally, they have a lot of experience in their specialized application field and hence can provide better software. In contrast, in-house programmers often have to work over a wide range of application areas; they may not be possessing expertise for undertaking proposed software development.
 - (iv) **Cost:** Software vendors can leverage the cost of developing a product by selling the product to several other firms, thereby realizing a lower cost from each application user. Thus, a pre-written application package generally costs less than an in-house developed package. In addition, many hidden costs are faced by organisations that want to develop applications in-house. Hence, application

packages, sometimes, turn out to be cheaper compared to in-house developed software.

(c) **Evaluation of the new system:** The final step of the system implementation is evaluation. Evaluation provides the feedback necessary to assess the value of information and the performance of personnel and technology included in the newly designed system. This feedback serves two functions:

1. It provides information as to what adjustments to the information system may be necessary.
2. It provides information as to what adjustments should be made in approaching future information system development projects.

There are two basic dimensions of information systems that should be evaluated. The first dimension is concerned with whether the newly developed system is operating properly. The other dimension is concerned with whether the user is satisfied with the information system with regard to the reports supplied by it.

Development evaluation: Evaluation of the development process is primarily concerned with whether the system was developed on schedule and within budget. This is a rather straightforward evaluation. It requires schedules and budgets to be established in advance and that record of actual performance and cost be maintained. It may be noted that very few information systems have been developed on schedule and within budget. In fact, many information systems are developed without clearly defined schedules or budgets. Due to the uncertainty and mystique associated with system development, they are not subjected to traditional management control procedures.

Operation evaluation: The evaluation of the information system's operation pertains to whether the hardware, software and personnel are capable to perform their duties and they do actually perform them so. Operation evaluation answers such questions:

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. For example, if the systems analyst lays down the criterion that a system which is capable of supporting one hundred terminals should give response time of less than two seconds, evaluation of this aspect of system operation can be done easily after the system becomes operational.

Information evaluation: An information system should also be evaluated in terms of information it provides. This aspect of system evaluation is difficult and it cannot be

conducted in a quantitative manner, as is the case with development and operation evaluations. The objective of an information system is to provide information to support the organizational decision system. 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. User satisfaction can be used as a measure to evaluate the information provided by an information system. Measurement of user satisfaction can be accomplished using the interview and questionnaire technique. If management is generally satisfied with an information system, it is assumed that the system is meeting the requirements of the organization. If management is not satisfied, modifications ranging from minor adjustments to complete redesign may be required.

Question 5

- (a) Write a detailed note on the expectations, fears and the ground realities that a corporate management faces during the post-implementation phase of ERP. (10 marks)
- (b) What do you understand by ON-LINE, REAL-TIME SYSTEMS ? (5 marks)
- (c) For an On-line, Real-time sales order processing system, draw the systems flow chart. (5 marks)

Answer

- (a) Most of the post-implementation problems of ERP can be traced to wrong expectations and fears. Sometimes it is also due to the ERP vendors and their pre-implementation sales hype. Popular expectations are :
 - An improvement in processes,
 - Increased productivity on all fronts,
 - Total automation and disbanding of all manual processes,
 - Improvement of all key performance indicators,
 - Elimination of all manual record keeping,
 - Real time information system available to concerned people on a need basis,
 - Total integration of all operations.

ERP software attempts to integrate all departments and functions across the enterprise onto a single computer system that serves the individual requirements of different departments. Instead of having discreet systems for finance and HR, it provides a common system for all. So if required, the materials department can view pending orders and instantly calculate the quantity of raw materials to be purchased. This keeps inventory levels within safe limits and hence controls costs. While all this may sound like a silver bullet to enterprises, ERP has gone sour for many companies in the past. The

problems have been primarily with integration. Also, the software required people to change their business processes too drastically.

An ERP implementation impacts people, systems, and the organization as a whole and barriers are expected from these areas since work processes are expected to be altered when ERP is introduced. Business processes, roles, and responsibilities undergo change. And when this happens, the organizations encounter a sticky issue called 'resistance to change'.

In the evaluation stage, users should articulate their business requirements and see whether a particular ERP solution meets their needs. This way one can close the gap between what the package offers and the business requirements. Implementation should not begin without this. Often, employees have high expectations and think ERP will solve most business problems. It is necessary to make realistic and accurate expectations before embarking on an ERP project. This is addressed by preparing a project charter stating the realistic expectations, and key performance parameters to be focused on during the project, and project measurement. Having defined this, it is necessary to communicate this to the stakeholders in the ERP project.

Some of the fears on ERP implementations are :

- Job redundancy.
- Loss of importance as information is no longer an individual prerogative.
- Change in job profile:
- An organizational fear of loss of proper control and authorization.
- Increased stress caused by greater transparency.
- Individual fear of loss of authority.

Since ERP introduces transparency in operations and brings about more discipline, people who are empowered are bound to oppose it. People who are very used to a particular system or a certain set of processes, would not accept an alternative like ERP so easily and would not adapt to the new system. Change management is about handling the issues arising due to differences in legacy processes/ systems and the new ERP system. Business processes may have to be re-engineered for ERP, something that is bound to draw disapproval, especially from function heads.

Balancing the expectations and fears is a very necessary part of the implementation process. The ground realities are:

- Changing the organization involves three levers-strategies, business process and change, and consequential organization change.
- In most companies in India, many process related key performance indicators have not been measured till now, either because the company did not feel it necessary or lacked the tools to do so. Measuring such indicators brings in new culture.

- The genetic nature of the ERP packages is such that there would be processes peculiar to some sectors and organizations, which may have to be kept out of the process.
- Some of the processes are better done manually.

ERP should be treated as a business project—not an IT project driven by the Information Systems. Changing the organization requires mindset change. Without a willingness to change, it would be a classic case of an old organization plus new technology leading to an expensive old organization. So, it is important to get the involvement of the function heads and top business executives. An organization must also be prepared for ERP and be clear about its requirements. This necessitates knowing the business objectives and goals, and mapping the processes to these. ERP is just the enabler that automates the entire process. The objectives for ERP must also be identified, documented, and communicated.

A successful ERP implementation is not the end of the road as far as change is concerned, and continuous improvements are required to reap the benefits. The expectations, fears and reality can most obviously be balanced during the process of implementation itself.

- (b) An **on-line real time (OLRT)** system processes a transaction as soon as it is entered. Practically, no delays occur during computer processing. The transaction recording and entry system may be created at the point of sale (POS) in the machine-readable form and entered directly into the computer. A system can be fully automated, and even the delay in entering the transaction could be eliminated.

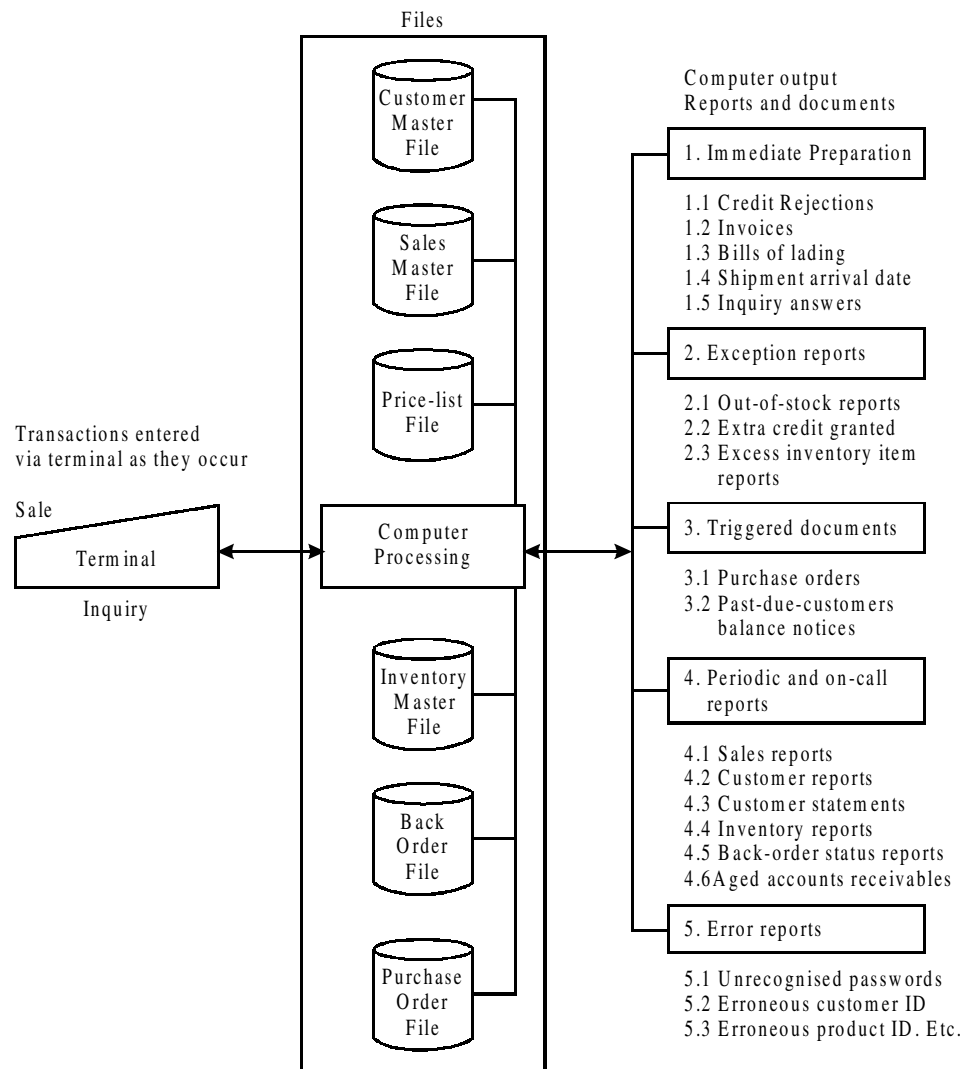
In an OLRT system, all files of the sub-systems related with a particular type of transaction processing must be electronically connected to the computer when a transaction of that type is entered into the machine. Generally, the files of an OLRT system reside on magnetic disks.

The OLRT systems operate (processing) entirely in a different manner compared to BATCH systems. In Batch systems, the transactions for a pre-defined period say a day, a week or a month are collected and then processed in one go. Whereas in OLRT systems, transactions are processed as and when they are created. These days, even the transactions can be created on telephone lines; e-mails, faxes etc. and the processing takes place without losing any time.

OLRT systems are very useful for enquiries. In Bank applications, the customer may be interested to know about the balance of his account, which may be either known through a telephone or directly by a machine, after entering few details.

In an OLRT system, there may be few user-input controls. Extensively programmed edit and logging controls are required to protect the computer files from erroneous or unauthorized transactions. It is also essential for important printed reports, such as control reports, exemption reports, or summaries, to be carefully reviewed by a user department employee who is not responsible for entering transactions.

(c) The system flow chart for an On-line, Real-time Sales order processing system is drawn as under:



Question 6

- (a) *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 ?* (5+5 = 10 marks)
- (b) *Give an example of an Information Security Policy Statement.* (10 marks)

Answer

- (a) There is no doubt that there has been a steep rise in the **Internet computer frauds**. This is mainly due to a number of characteristics of Internet, which are likely to attract fraudsters to commit frauds.
- (i) It is unregulated in so far as who may set up a site. No license fees are payable to any central authority and no form of vetting is, or in practical terms ever could be, carried out on those persons or entities setting up sites.
 - (ii) An Internet site can be set up anywhere in the world at very low cost and can be reached from anywhere else in the world at low cost.
 - (iii) An impressive site with links to established companies or financial institutions may be more than an empty shell designed to attract and trap the unwary. There is no easy way of separating the genuine from the false.
 - (iv) The glamour and novelty of the Internet and the spurious credibility claimed by a site may cause otherwise prudent investors to become involved in fraudulent schemes.
 - (v) A site may, and probably will, operate outside the legal jurisdiction of the country in which the victim of the fraud resides.

The above factors make it extremely difficult to discover, in sufficient time to effect recovery or at all, the identity of the WWW Site operator.

Frauds on the Internet are proliferating as is evident by the examples released in the press.

- (i) The offices of a small Illions company created the Agency for Inter-American Finance on the WWW in late 1995. The WWW site boasted impressive graphics and was linked to the Internet by a Swiss Internet Service provider. AIF claimed to be based in Antigua and that it was a provider of investment capital for Latin American businesses. Later investigation revealed that AIR was a Panamanian shell company, and that the bond and guarantor were fake.
- (ii) "Fortuna Alliance" offered investors a return of \$5,000 per month for an investment of \$250. The USFTC began an investigation against this company for this improbable scheme. But then the investors had already lost \$6 million before FTC blocked access to the site.
- (iii) European Union Bank, which traded over the Internet, collapsed.

These are some common examples of Internet frauds:

- **Overpayment Scam:** In this very common scam type, a buyer will contact the seller and negotiate a deal on the merchandise. Many times, this buyer is located outside the country, and may be acting as a "broker" or a "third party" on behalf of another interested party. The buyer will send a cashier's cheque (or money order) for more than the asking price of the merchandise. The buyer will instruct the seller to send the difference for the overpayment. Unfortunately, the cashier's cheque or money order used to originally pay the buyer is counterfeit and will be returned to the seller with insufficient funds. The seller is then cheated out of his or her own cash, plus any merchandise that was sent.
- **Wire Fraud:** In this scam, the buyer will request permission to wire transfer money directly into the seller's bank account. By providing confidential bank account information to the buyer, seller's account may be compromised by unscrupulous parties. Companies should always use caution when providing any form of personal information.
- **Customs Scams:** There are recent reports from the IFCC involving Eastern European countries and high incidences of fraud. Many of the fraudulent buyers of items are located in these countries and often ask that the seller to ship in a manner that will avoid customs or taxes. Sellers should be wary of this type of behavior.

Even though there is an increase in Internet computer frauds, not many are reported for various reasons and many companies are unable to contain it due to following reasons:

- (i) Not everyone agrees on what constitutes computer fraud.
 - (ii) Many computer frauds go undetected.
 - (iii) 80-90% of the frauds data that are uncovered are not reported. Only the banking industry is required by law to report all frauds.
 - (iv) Most networks have a low level of security. It is estimated that two out of three sites have serious vulnerabilities, and most firewalls and other protective measures at the sites are ineffective.
 - (v) Many Internet pages give step-by-step instructions on how to perpetrate computer frauds and abuses. There are also thousands of pages on how to break into routers and disable web servers.
 - (vi) Law enforcement is unable to keep up with the growing number of computer frauds.
- (b) The purpose of the information security policy is to protect the organization's information assets from all types of threats, whether internal or external, deliberate or accidental. Information system security is critical to the organisation's survival.

A typical Information Security Policy Statement should ensure that

- ◆ Assets will be classified as to the level of protection required;
- ◆ Information will be protected against unauthorized access;

- ◆ Confidentiality of information will be assured;
- ◆ Integrity of information will be maintained;
- ◆ Personnel security requirements will be met;
- ◆ Physical, logical and environmental security (including communications security) will be maintained;
- ◆ Legal, regulatory, and contractual requirements will be met;
- ◆ Systems development and maintenance will be performed using a life cycle methodology;
- ◆ Business continuity plans will be produced, maintained, and tested;
- ◆ Information security awareness training will be provided to all staff;
- ◆ All breaches of information system security, actual or suspected, will be reported to, and promptly investigated by Information Systems Security;
- ◆ Violations of Information Security Policy will result in penalties or sanctions;
- ◆ Standards, practices, and procedures will be produced, and measures implemented to support the Information Security Policy. These may include, but are not limited to, virus protection, passwords, and encryption;
- ◆ Business requirements for the availability of information and information systems will be met;
- ◆ The roles and responsibilities regarding information security are defined for:
 - Executive management;
 - Information systems security professionals;
 - Data owners;
 - Technology providers;
 - Users;
 - Information systems auditors.
- ◆ The Information Systems Security function has direct responsibility for maintaining the Information Security Policy and providing guidance and advice on its implementation;
- ◆ All managers are directly responsible for implementing the Information Security Policy within their areas of responsibility, and for adherence by their staff; and
- ◆ It is the responsibility of each employee to adhere to the Information Security Policy.

Question 7

Write short notes on the following:

- (a) *Strategic and Tactical decisions*
- (b) *Business Process Re-engineering*
- (c) *Encryption*
- (d) *System Development Life-cycle.* (4×5 = 20 marks)

Answer

- (a) **Strategic and Tactical Decisions:** Decisions made at the strategic level of the organization to handle problems critical to its survival and success are called strategic decisions. They have a vital impact on the direction and functioning of the organization. Some of the examples are decision on plant location, introduction of new products, making major new fund – raising and investment operations, adoption of new technology etc. Much analysis and judgment go into making strategic decisions. Strategic decisions are made under conditions of partial knowledge and generally can not be programmed.

Tactical level decisions are to be taken by middle level of managerial hierarchy. At this level, managers plan, organize, lead and control the activities of other managers. A single strategic decision calls for a series of tactical decisions, which are of a relatively structured nature. Tactical decisions are relatively short, step-like spot solutions to breakdown strategic decisions into implementable packages.

The other features of tactical decisions are; they are more specific and functional; they are made in a relatively closed setting; information for tactical decisions is more easily available and digestible; they are less surrounded by uncertainty and complexity; decision variables can be forecasted and quantified without much difficulty and their impact is relatively localized and short-range. Tactical decisions are made with a strategic focus.

The distinction between strategic and operational decisions could be high-lighted by means of an example. Decisions on mobilisation of military resources and efforts and on overall deployment of troops to win a war are strategic decisions. Decisions on winning a battle are tactical decisions.

As in the case of programmed and non-programmed decisions, the dividing line between strategic and tactical decision is thin. For example, product pricing is tactical decision in relation to the strategic decision of design and introduction of a new product in the market. But product pricing appears to be a strategic decision to down-line tactical decisions on dealer discounts.

- (b) **Business Process Reengineering (BPR):** ERP is a result of a modern Enterprise's concept of how the Information System is to be configured to the challenging environments of new business opportunities. However, merely putting in place an information system is not enough. Every company that intends to implement ERP has to re-engineer its processes in one form or the other. This process is known as Business

Process Reengineering (BPR). BPR is the fundamental rethinking and radical redesign of processes to achieve dramatic improvement in critical, contemporary measure of performance such as cost, quality, service and speed.

Radical Redesign means BPR is reinventing and not enhancing or improving. According to BPR philosophy, whatever was being done in past, it was all wrong, so one has to reassemble the new system to redesign it afresh. There is no point in simplifying or automating a business process, which does not add any value to the customer; such business processes should be eliminated altogether.

BPR aims at major transformation of the business processes to achieve dramatic improvement. Here, the business objectives of the enterprise such as profits, customer – satisfaction through optimal cost, quality, deliveries etc. are achieved by transformation of the business processes which may, or may not, require the use of IT.

The concept of BPR when merges with the concept of IT, the business engineering emerges, which is the rethinking of Business Processes to improve speed, quality and output of materials or services. In other words, business engineering is the method of development of business processes according to changing requirements.

- (c) **Encryption:** Encryption refers to conversion of data into a 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, the cipher text is decoded (decrypted) back into clear text. The encryption algorithm uses a key, which is a binary number that is typically from 56 to 128 bits in length. The more bits in the key, the stronger the encryption method. Today, nothing less than 128 bit algorithms are considered truly secure. Two general approaches to encryption are private key and public key encryption.

Private Key Encryption: Data encryption standard (DES) is a private-key encryption technique designed in the early 1970s by IBM. The DES algorithm 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, which is used to produce a cipher text message. The message enters the communication channel and is transmitted to the receiver's location, where it is stored. The receiver decodes the message with a decryption program that uses the same key employed by the sender.

Public Key Encryption: The public key encryption technique uses two different keys: one for encoding messages and the other for decoding them. Each recipient has a private key that is kept secret and a public key that is published. The sender of a message uses the receiver's 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 it may fall into the hands of criminal.

- (d) **System Development Life Cycle:** The process of system development starts when management realise that a particular business needs improvement. The system

development life cycle method can be thought of as a set of activities that analysts, designers and users carry out to develop and implement an information system.

The system development life cycle method consists of the following activities:

- (i) **Preliminary investigation:** It is undertaken when users come across a problem or opportunity and submit a formal request for a new system to the MIS department. This activity consists of three parts; request clarification, feasibility study and request approval.
- (ii) **Requirements analysis or systems analysis:** In this stage, the analysts work closely with employees and managers of the organization for determining the information requirements of the users. Several fact-finding techniques and tools such as questionnaires, interviews, observing decision-maker behaviour and office environment, etc. are used for understanding the requirements of the users. As details are gathered, the analysts study the present system to identify its problems and shortcomings and identify the features which the new system should include to satisfy the new or changed user application environment.
- (iii) **Design of the system:** It produces the details that state how a system will meet the requirements identified in the previous step. The analyst designs various reports/outputs, data entry procedures, inputs, files and database. He also selects file structures and data storage devices. These detailed design specifications are then passed on to the programming staff for software development.
- (iv) **Acquisition and development of software:** In this stage, resource requirements such as specific type of hardware, software and services are determined. Subsequently, choices are made regarding which products to buy or lease from which vendors. Software developers may modify and then install purchased software or they may write new custom designed programs.
- (v) **System testing:** Before the information system can be used, it must be tested. Special test data are input for processing, and results are examined. If it is found satisfactory, it is eventually tested with actual data from the current system.
- (vi) **Implementation and maintenance:** After system is found to be fit, it is implemented with actual data. After implementation, the system is maintained; it is modified to adapt to changing users and business needs.