PAPER – 6 : MANAGEMENT INFORMATION AND CONTROL SYSTEMS

Question No. 1 is compulsory.

Answer any four questions from remaining six questions.

Question 1

(a) Why Computerised Information systems are more vulnerable to many more kinds of threats than manual systems? Name some of the key areas where large amounts of data stored in electronic form are most vulnerable.

(b) Discuss some common types of field interrogation as a validation control procedure in an EDP set up.

(c) Differentiate between General and Application controls. Also mention the broad categories into which the first can be subdivided.

(d) How does MIS auditing enhance the control process? (5 + 5 + 5 + 5 = 20 Marks)

Answer

(a) When large amounts of data are stored in electronic form they are vulnerable to many more kinds of threats than when they exist in manual form. Since the data is in electronic form and many procedures are invisible through automation, Computerized Information Systems (CIS) are vulnerable to destruction, misuse, error, fraud, hardware and software failures. Online systems and those utilizing the Internet are especially vulnerable because data and files can be immediately and directly accessed through computer terminals at many points in the network. Hackers can penetrate corporate networks and cause serious system disruptions. Computer viruses can spread rampantly from system to system, clogging computer memory or destroying programs and data. Software presents problems because of high costs of correcting errors and because software bugs may be impossible to eliminate. Data quality can also severely impact system quality and performance.

Following are the key areas due to which data stored in electronic form are most vulnerable:

(1) Hardware failure,	(2) Software failure,
(3) Personnel actions,	(4) Terminal access penetration
(5) Theft of data, services, equipment,	(6) Fire
(7) Electrical problems,	(8) User errors
(9) Program changes,	(10) Telecommunication problems

(b) Some common types of field interrogation as a validation control procedure in an EDP set up are discussed below:

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

(2) Picture checks: These check against entry of incorrect characters into processing.

(3) Valid Code Checks: Checks are made against predetermined transactions codes, tables or other data to ensure that input data are valid. They may either be embedded in the programs or stored in files.

(4) Check digit: It is an extra digit that is added to the code when it is originally assigned. It allows the integrity of the code to be established during subsequent processing.

(5) Arithmetic Checks: Arithmetic is performed in different ways to validate the result of other computations of the values of selected data fields.

(6) Cross Checks: It may be employed to verify fields appearing in different files to check that the results tally.

(c) General controls apply to a wide range of exposures that systematically threaten the integrity of all applications processed within CBIS environment. Application controls are focused on exposures associated with specific systems such as payroll, accounts receivable etc. These controls help to ensure the completeness and accuracy of transaction processing, authorization, and validity.

General controls can be subdivided under following headings:

(1) Operating system controls

(2) Data managements Controls

(3) Organizational structure controls

(4) Systems development controls

(5) Systems maintenance controls

(6) Computer Centre security controls

(7) Internet and intranet controls

(8) Personal computers control.

(d) Comprehensive and systematic MIS auditing can help organizations to determine the effectiveness of the controls in their information systems. Regular data quality audits should be conducted to help organizations ensure a high level of completeness and accuracy of the data stored in their systems. Data cleansing should also be performed to create consistent and accurate data for company wide use in e-commerce and e-business.

An MIS audit identifies all of the controls that govern individual information systems and assesses their effectiveness. To accomplish this, the auditors must acquire a thorough understanding of operations, physical facilities, telecommunications, control system, data security objectives, organizational structure, manual procedures and individual applications.

The auditor usually interviews key individuals who use and operate specific information system concerning their activities and procedures. Applications controls, overall integrity controls and control discipline are examined. The auditor should trace the flow of sample transactions through the system and perform tests using, if appropriate, automated audit software.

The auditor lists and ranks all control weaknesses and estimates the probability of their occurrences. He then assesses the financial and organisational impact of each threat. Management is expected to device a plan for countering significant weaknesses in controls.

Question 2

(a) State the factors to be considered for designing an effective Management Information System.

(b) Enumerate various information which are required for sales support and sales analysis.

(10 + 10 = 20 Marks)

Answer

(a) 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 such 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 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 be established using a manual system. 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.

(b) Information requirements for sales support and sales analysis are enumerated below:

   (i) Sales support: A specialized sales support information system must provide the following information to sales personnel:

   - Products descriptions and performance specifications.
   - Product Prices.
   - Quantity discounts and other product discount information.
   - Sales incentives for salespersons.
   - Sales promotions.
   - Financing plans for customers.
   - The strengths and weaknesses of competitors' products.
   - The histories of customers ' relations with the company.

- Sales policies and procedures established by the company.
- Products that have not yet been introduced.
- Products' inventory levels.
- Buying habits of consumers.

These and other information come from a variety of sources. Product performance specifications, for example, may come from the engineering department.

(ii) Sales Analysis:

To keep abreast with the competitors in the market, the sales analysis is a very vital activity. It must provide the following information:

- Sales trends (product-wise)
- Product wise profitability
- Region, branch wise sales performance
- Sales person wise performance

The above information is derived from Sales Transaction Processing System as well as from other systems like Financial Accounting System and HR Management System etc. The majority of information comes from actual sales transactions and is contained on sales invoices. To fully support the sales analysis system, invoices should contain information about product type, product quality, price discount terms, customer identity and type, sales region, and salesperson.

Information from other sources should also be included in the sales reports. Specifically, the sales reports must contain information about the profitability of products, product lines, sales territories, and individual sales persons. Profitability reporting requires information about product administrative and selling costs.

Question 3

(a) What are the project management items associated with an I.T. project system failures? Give the elements to be included in the adopted framework to avoid such failures.

(b) Discuss some of the commonly used coding schemes.

(c) Describe Bench marking problem on vendor's proposal. (10 + 5 + 5 = 20 Marks)

Answer

(a) Items associated with IT project system failure are as follows:

(i) Underestimation of the time to complete the project.

(ii) Senior management did not monitor the project closely enough.

(iii) Underestimation of necessary resources.

(iv) Size and scope of the project underestimated.

(v) Inadequate project control mechanism.

(vi) Systems specifications kept changing.

(vii) Inadequate planning.

Elements to be included in the framework to avoid such failures are as stated below:

(i) User participation in defining and authorizing the system.

(ii) Assignment of appropriate staff to the system development and definition of their responsibilities and authorities.

(iii) A clear written statement of system nature and scope.

(iv) A feasibility study that is the basis of senior management approval to proceed with the system.

(v) A system master plan, including realistic time and cost estimates for control of the system.

(vi) A risk management program to Identify and mange risks associated with each project.

(vii) Division of the system into manageable processes often called phases.

(viii) Approval of work accomplished in one phase before working on the next phase.

(ix) Integration of the quality assurance plan including the systems development cycle (SDLC) methodology with the system master plan.

Project management, particularly the planning process and establishing the project schedule can ultimately determine the success of the project.

(b) Some of the commonly used coding schemes are discussed below:

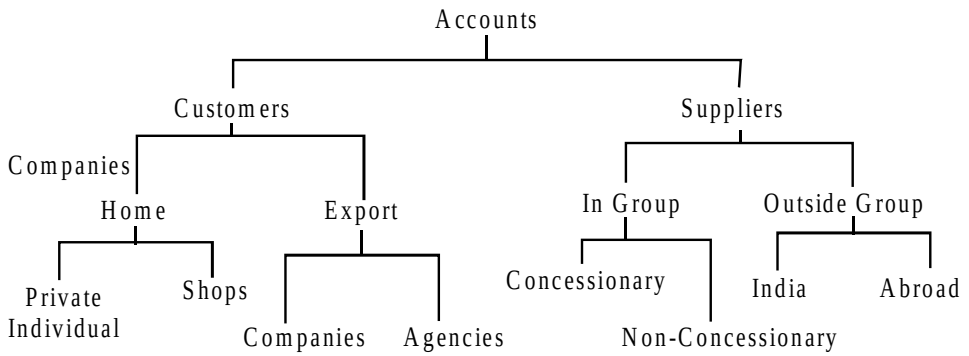
(1) Classification codes: They place separate entities such as events, people or objects into distinct groups called classes. A code is used to distinguish one class from another. The code is recorded on the source document by the user. In an online system, it can be keyed directly in the system through a terminal. The user classifies the event into one of the several categories and records the code. Classification codes vastly simplify the input process because only a single digit code is required.

(2) Function Codes: These codes state the activities or work to be performed without spelling out all the details in narrative statements. Analysts use this type of codes frequently.

(3) Significant digit Subset Codes: Suppose item numbers are to be assigned to the different materials and products that a firm stocks or sells. Then numbers are assigned in sequence from the first to the last or a prefix can be added to the identification numbers. Codes can be divided into subsets or sub codes, characters that are part of the identification number and that have special meaning. Using digits in an identification number to convert additional information does not add to the length of the data but provides invaluable information to the management.

(4) Mnemonic Codes: These are suitable where the codes have to be remembered by the people.

(5) Hierarchical Classification:



This classification can be developed for use in almost any business and for all kinds of office records.

(c) Bench Marking Problem: Benchmarking problems for vendors' proposals are sample programs that represent at least a part of the buyer's primary computer work load. They include software considerations and can be current applications programs or new programs that have been designed to represent planned processing needs i.e., benchmarking problems are oriented towards testing whether a computer offered by the vendor meets the requirements of the job on hand of the buyer. They are required to be representative of the job mix of the buyer. Obviously, benchmarking problems can be applied only if job mix has been clearly specified. The benchmarking problems, would then comprise long jobs, short jobs, tape jobs, disk jobs, mathematical problems, input and output loads etc, in proportion typical of the job mix. If the job is truly represented by the selected benchmarking problems, then this approach can provide a realistic and tangible basis for comparing all vendors' proposals. Tests should enable buyer to effectively evaluate cross performance of various systems in terms of hardware performance (CPU and input/output units), compiler language and operating system capabilities, diagnostic messages, ability to deal with certain types of data structures and effectiveness of software utilities.

Bench marking problems, however, suffer from a couple of disadvantages. It takes considerable time and effort to select problems representative of the job mix which itself must be precisely defined. It also requires the existence of operational hardware, software and services of systems. Nevertheless, this approach is very popular because it can test the functioning of vendor's proposal. The manager can extrapolate in the light of

the results of bench marking problems, the performance of the vendors' proposals on the entire job mix.

Question 4

(a) Describe the sequence of events which occur immediately for each transaction when controlled by the sales order entry computer programs in an OLRT system.

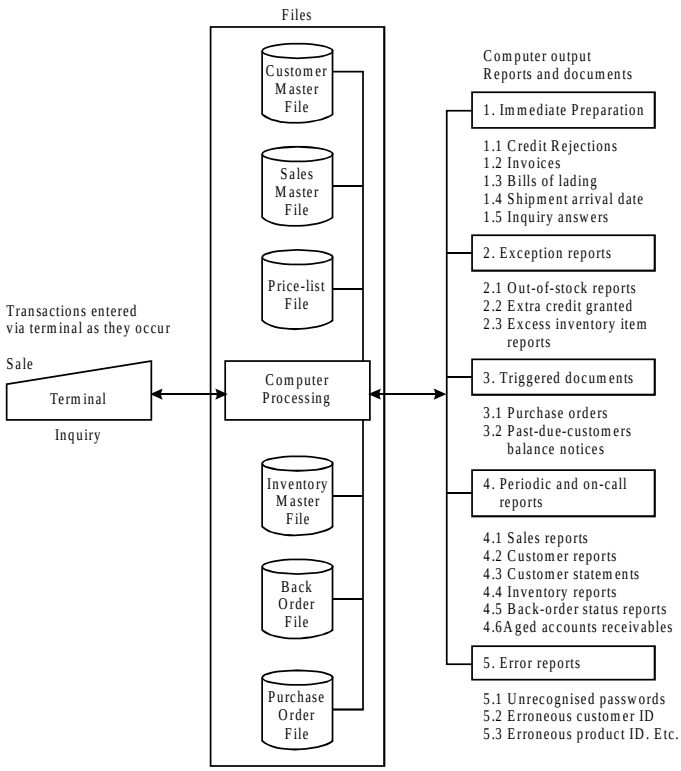
(b) Why is personnel training important? What type of training should be imparted to users?

(c) How can computer fraud be committed using input in four different ways?

(10 + 5 + 5 = 20 Marks)

Answer

(a) Sales order processing system: Controlled by the sales order entry computer programs in an OLRT systems, the following events occur immediately for each transaction in the sequence given below :



1. The sales person tells the computer the nature of the transaction by entering a transaction code identifying it as a credit sales transaction; this activates the sales

order processing computer program. The customer number, the item number and quantity are then entered.

2. The computer program checks the customer's account in the customer file to "validate" the customer number (to establish that a credit customer exists with that number) and to see how much additional credit the customer can be granted; the up-to-date credit status of the customer is contained in the customer's account. If the customer cannot be extended further credit, the salesperson is notified by the computer and the credit transaction is cancelled.

3. The product number of the product ordered is checked for validity in the inventory file, and the stock level of that item shown by the inventory file is compared with the number of items ordered. If there is an insufficient quantity of a product, the program examines the purchasing file to establish when the next shipment is due. The system conveys this information to the terminal of the salesperson and awaits further instructions. The salesperson consults with the customer and then cancels the order for that item or changes the order to the quantity available and back-orders the additional items desired, according to the customer's wishes.

4. The computer program then seeks product pricing and quantity discount information from the price list file and special "preferred customer" discount information, if any, from the customer file. The total cost of the item to the customer including tax is calculated by the computer.

5. The details of the transaction, including the cost details, may appear on a display device at the salesperson's terminal so that they can be told to the customer. Changes may be made in the order by the customer and entered into the computer. The salesperson signals the computer when the customer approves the transaction.

6. An invoice is printed out for mailing, either at the salesperson's terminal or on a printer at a central location.

7. On a printer at the warehouse location of the merchandise, the computer system prepares a multipart-shipping document, which is the authorisation for shipping personnel to select, pack, and ship the merchandise ordered. One copy of the document, known as the "bill of lading" is enclosed and shipped with the merchandise.

8. Product records in the inventory file are adjusted to reflect the decrease in inventory caused by the sale.

9. The customer's account is updated to reflect the details of the transaction, and a new customer balance is calculated and placed in the account.

10. The record for each item in the sales file is updated with details of the transaction. This updating may include all details necessary for sales analysis based on customer type and territory, as well as other factors. A separate transaction listing that records all details of the entire transaction in one transaction file (not shown) may also be made for control and backup purpose.

(b) Personnel training: A system can succeed or fail depending on the way it is operated and used. The quality of training received by the personnel involved with the system in various capacities helps or hinders the successful implementation of information system. Thus, training is a major component of systems implementation.

When a new system is acquired which often involves new hardware and software, some type of training is needed. Users must be instructed first how to operate the equipment. The training must also instruct individuals involved in trouble shooting of the system, determining whether the problem is caused by the equipment or software or by something they have done in using the system. Training in data coding emphasizes the methods to be followed in capturing data from transactions or preparing data for decision support activities. Users should be trained on data handling activities such as editing data, formulating inquires and deleting records of data. They will have to prepare disks, load paper into printers or change ribbons on printers, format and test the disk.

(c) The simplest and most common way to commit a fraud is to alter computer input. In collusive fraud, one perpetrator, for example, opened an account at a bank and then prepared blank deposit slip. The slips were similar to those available in bank lobby, with his account number encoded. One morning he replaced all the deposit slips in the bank lobby with his forged ones. For three days all bank deposits using the forged slips went directly into his account. Then he withdrew the money and disappeared.

In disbursement frauds, the perpetrator can cause a company to either pay too much for ordered goods or to pay for goods that are never ordered. He may keep the amount low enough so that most companies may not bother for purchase orders or approvals for such small amounts.

To commit payroll frauds, perpetrator can enter data to increase that salary, create a fictitious employee or retain a terminated employee on records and proceeds to intercept and cash the illegal cheques.

In a cash receipt fraud, the perpetrator may hide the theft by falsifying system input e.g. he may sell full-price tickets but enter the sale as half-price tickets and pocket the difference.

Question 5

(a) Describe some of the powers of the Cyber Appellate Tribunal.

(b) What are the five different levels of integration of CASE tools?

(c) What are the subversive threats? How do the intruders manipulate the messages being transmitted? (5 + 5 + 10 = 20 Marks)

Answer

(a) Powers of the Cyber Appellate Tribunal: Section 58 of the Information Technology Act 2000 provides for the procedures and powers 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:

(i) Summoning and enforcing the attendance of any person and examining him on oath.

(ii) Requiring production of documents and other electronic records.

(iii) Receiving evidence on affidavits.

(iv) Reviewing its decisions.

(v) Issuing commissions for examination of witness etc.

(b) There are five different levels of integration of CASE tools as stated below:

(1) Platform integration: Here the tools to be implemented run on the same platform where platform means either a single computer/operating system or a network of system.

(2) Data integration: It is the process of exchange of data by CASE tools. The result from one tool can be passed on as input to other tools.

(3) Presentation integration: It means that the tools in the system use a common metaphor or style and a set of common standards for user interaction.

(4) Control Integration: It is the mechanism of one tool in a workbench or environment to control the activation of other tools in the CASE system.

(5) Process integration: This means that the CASE system has embedded knowledge about the process activities, their phasing, their constraints and the tools needed to support their activities.

(c) Subversive threats refer to a situation where an intruder attempts to violate the integrity of some components in the subsystem. By installing an invasive tap on communication line, he can read and modify data or through inductive tap, he can monitor electromagnetic transmissions and allow the data to be read only. Subversive attacks can provide intruders with important information about messages being transmitted.

The intruders can manipulate messages in following ways:

(i) Intruders may insert a message in a message stream being transmitted e.g. EFTs add transfer of funds in an additional account.

(ii) They may delete a message being transmitted, e.g. remove a/c withdrawal message.

(iii) They may modify the contents of message e.g. increase the amount filled in a deposit transaction.

(iv) Intruders may alter the order of the message in a message stream.

(v) They may duplicate message in a message stream, or copy deposit transactions for their accounts.

(vi) They may deny message services between a sender and a receiver by discarding messages or delaying messages.

(vii) They may use techniques to establish spurious associations so that they are regarded as legitimate users of a system. They may play back a handshaking sequence previously used by a legitimate user of the system.

Question 6

Please read carefully the following three scenarios and answer the questions given below:

(a) Scenario 1 :

Nobody told you that your Internet use in the office was being monitored. Now you have been warned you will be fired if you use the Internet for recreational surfing again. What are your rights?

(b) Scenario 2 :

Your employees are abusing their Internet privileges, but you don't have an Internet usage policy. What do you do?

(c) Scenario 3 :

Employee Mr. X downloads adult material to his PC at work, and employee Miss Y sees it. Miss Y then proceeds to sue the company for sexual harassment. As the employer, are you liable? (5 + 7 + 8 = 20 Marks)

Answer

(a) Scenario 1: When you are using your office computer, you have virtually no rights. You would have a tough time convincing the court that the boss invaded your privacy by monitoring your use of the company PC during office hours. You should probably be grateful that you only got a warning stating that you will be fired if you use the Internet for recreational surfing again .

(b) Scenario 2: Although the law is not fully developed in this area, courts are taking a straightforward approach. If it is a company computer, the company can control the way in which it is to be used by its employees. You really don't need an Internet usage policy to prevent inappropriate use of your company's computer. To protect the company in future, it is advisable to distribute an Internet usage policy to your employees as soon as possible to stop your employees from abusing their Internet privileges.

(c) Scenario 3: Whether it comes from the Internet or from a magazine, adult material simply has no place in the office. So Miss Y could certainly sue the company for making her work in a sexually hostile environment. The best defense for the company is to have an Internet usage policy that prohibits employees to access adult sites. Of course, you have to follow-through and monitor. Today, software is available for monitoring the employees whenever they visit adult sites. It will shut down the computer and alert the person who is monitoring Internet usage. If someone is caught browsing adult material in the office, you must at least send a written communication to the offending employee. If the company lacks a strict Internet usage policy, Miss Y could prevail in the Court.

Question 7

Write short notes on the following:

(a) Enterprise Controlling

(b) Integrated Test Facility

(c) Restorative Information Protection

(d) Internet Frauds. (4 × 5 = 20 Marks)

Answer

(a) Enterprise Controlling: Enterprise can be managed by using an integrated enterprise management. This consists of getting accounting data prepared by subsidiaries for corporate reporting which will be automatically prepared simultaneously within the local books of each subsidiary. This data is transferred to a module called enterprise controlling (EC).

It is easy to transfer the data to the EC module to automatically set up consolidated financial statements including elimination of inter-company transactions currency translations etc. Enterprise controlling consist of 3 modules. EC-CS component is used for financial statutory and management consolidation. EC-PCA allows to work with internal transfer prices and at the same time to have the right values from company, profit centre and enterprise perspectives in parallel. It is also possible to take data directly from EC-PCA to ES-CS consolidation.

EC-EIS (Executive Information System) allows to take financial data from EC-PCA, EC-CS or any other application and combines with any external data such as market data, industry benchmark and / or data from non-SAP applications to build a company specific comprehensive enterprise information system.

EC allows to control the whole enterprise from a corporate and a business unit perspective within one common infrastructure. From EC-EIS top-level2 reports, end users can drill down to more detailed information within EC or any other R/3 application.

(b) Integrated Test Facility: It is one of the five concurrent audit techniques. It places a small set of fictitious records in the master files. The records might represent a fictitious division, department, or branch office, or a customer or supplier. Processing test transactions to update these dummy records will not affect the actual records. Because fictitious and actual records are processed together, company employees usually remain unaware that this testing is taking place. The system can distinguish ITF records from actual records, collect information on the effect of the test transactions and report the results. The auditor compares processing and expected results in order to verify that the system and its controls are operating correctly.

In a batch processing system, the ITF technique eliminates the need to reverse test transactions and is easily concealed from operating employees. ITF is well suited to testing on-line processing systems because test transactions can be submitted on a frequent basis. All this can be accomplished without disrupting regular processing operations. However, care must be taken not to combine dummy and actual records during the reporting process.

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

Planning and operating an effective and timely information backup and recovery program is vital to an operation. It does not simply involve backing up just the valuable information

but it frequently also means backing up the system as well, since the information may need services that the system provides to make the information usable.

The key requirement of any restorative information protection plan is that the information can be recovered. There is a common belief that if the backup program has written the information to the backup media, it can be recovered from the backup media. However, there are many variables that can prove that belief wrong.

Some of the questions that any restoratives information protection program must address are:

(i) Has the recovery process been tested recently?

(ii) How long did it take?

(iii) How much productivity was lost?

(iv) Did everything go according to plan?

(v) How much extra time was needed to input the data changes since the last back up?

(d) Internet frauds: With the fast changing and emerging Information Technology, the threat on information security is also increasing. One of the major threats is Internet Frauds. Whereas the Internet should be used for legitimate commerce and for business enhancement, its power is also being harnessed for criminal and fraudulent purposes. It attracts the fraudsters to make easy money because of:

- 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.
- An Internet site can be set up anywhere in the world at very low cost and can reach anywhere else in the world at low cost. This means that fraudsters now have “global reach” and can access a far larger market of potential victims than ever before. As fraudsters are always looking for new victims, this is a very attractive feature.
- An impressive site with links to established companies or financial institutions might be no more than an empty shell designed to attract and trap the unwary. There is no easy way of separating the genuine from the false.
- 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.
- A site may, and probably will, operate outside the legal jurisdiction of the country in which the victim of the fraud resides. A company which gives itself a UK Internet address may not have absolutely any legal or commercial connection with the jurisdiction.

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.