

MOCK TEST PAPER – 1
FINAL COURSE: GROUP – II
PAPER – 6: INFORMATION SYSTEMS CONTROL & AUDIT
SUGGESTED ANSWERS/HINTS

1. (a) **Systematic risks:** These are unavoidable risks; constant across majority of technologies and applications. For example, the probability of power outage is not dependant on the industry but is dependant on external factors. Systematic risks would remain, no matter what technology is used. Thus effort to seek technological solution to reduce systematic risks would essentially be unfruitful activity and needs to be avoided. Systematic risks can be reduced by designing management control process and does not involve technological solutions. For example, the solution to non availability of consumable is maintaining a high stock of the same. Thus a systematic risk can be mitigated not by technology but by management process. Hence, one would not make any additional payment for technological solution to the problem. To put in other words there would not be any technology linked premium that one should pay trying to reduce the exposure to systematic risk.

Unsystematic risks: These are the risks, which are peculiar to the specific applications or technology. One of the major characteristics of these risks would be that they can be generally mitigated by using an advanced technology or system. For example one can use a computer system with automatic mirroring to reduce the exposure to loss arising out of data loss in the event of failure of host computer. Thus by making additional investment one can mitigate these unsystematic risks.

- (b) **Delphi Approach:** This approach was first used by the Rand Corporation for obtaining a consensus opinion. Here, a panel of experts is appointed. Each expert gives his opinion in a written and independent manner. They enlist the estimate of the cost, benefits and the reasons why a particular system should be chosen, the risks and the exposures of the system. These estimates are then compiled together. The estimates within a pre-decided acceptable range are taken. The process may be repeated four times for revising the estimates falling beyond the range. Then a curve is drawn taking all the estimates as points on the graph. The median is drawn and this is the consensus opinion.

Scoring Approach: In the Scoring approach, the risks in the system and their respective exposures are listed. Weights are then assigned to the risk and to the exposures depending on the severity, impact on occurrence, and costs involved. The product of the risk weight with the exposure weight of every characteristic gives us the weighted score. The sum of these weighted score gives us the risk and exposure score of the system. System risk and exposure is then ranked according to the scores obtained.

(c) [Section 7] Retention of Electronic Records:

- (1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, -
 - (a) the information contained therein remains accessible so as to be usable for a subsequent reference;
 - (b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;
 - (c) the details, which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record:

However,

This clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

- (2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records. Publication of rules, regulation etc. in Electronic Gazette

(d) The detailed controls and objectives of access control are as follows:

- *Business requirement for access control:* To control access to information,
- *User access management:* To prevent unauthorized access to info systems,
- *User responsibilities:* To prevent unauthorized user access,
- *Network access control:* Protection of networked services,
- *Operating system access control:* To prevent unauthorized computer access,
- *Application Access Control:* To prevent unauthorized access to information held in information systems,
- *Monitoring System Access and use:* To detect unauthorized activities, and
- *Mobile Computing and teleworking:* To ensure information security when using mobile computing & teleworking facilities.

2. **(a)** The company, ABC Limited may face several new business risks when they migrate to real-time, integrated ERP systems. These risks include the following:
 - *Single point of failure* – All input data of an organization and transaction

processing is within one application system.

- *Structural Changes* - Significant personnel and organizational structural changes associate with reengineering or redesigning business processes.
- *Job Role Changes* - Traditional roles of users are changed to empowered-based role. They have more chances to access enterprise information in real-time. This point of control shifts from the back-end financial processes to the front-end point of creation.
- *Online Real-Time* – This environment requires a continuous business interaction. This warrants the capabilities of utilizing the ERP application and responds quickly to any problem that requires a re-entry of information (e.g., if field personnel are unable to transmit orders from handheld terminals, customer service staff may need the skills to enter orders into the ERP system correctly so the production and distribution operations will not be adversely impacted).
- *Change Management* - It is challenging to bring together a highly integrated environment when different business processes have existed among business units for long. The level of user acceptance of the system has a significant influence on its success. Training and awareness of users is mandatory, to understand that their actions or inaction have a direct impact upon other users and in the performance of their day-to-day duties.
- *Distributed Computing Experience* - Inexperience with implementing and managing this kind of environment may pose significant challenges.
- *Broad System Accessibility* – Increased remote access by users and outsiders and high integration among application functions allow increased access to the application and data.
- *Dependency on External Assistance* – Organization accustomed to in-house legacy systems may find that they have to rely on external help. Unless such external assistance is properly managed, it could introduce an element of security and resource management risk that may expose the organizations to a greater risk.
- *Program Interfaces and Data Conversions*–Extensive interfaces and data conversions from legacy systems and other commercial software are necessary. The exposures of data integrity, security and capacity requirements for ERP are much higher.
- *Audit Expertise* – Specialist expertise is required to effectively audit and control an ERP environment. The relative complexity of ERP systems has created specialization such that each specialist may know only a relatively small fraction of the entire ERP's functionality in a particular core module, e.g.

FI auditors, who are required to audit the entire organization's business processes, have to maintain a good grasp of all the core modules to function effectively.

- *Single sign on* - It reduces the security administration efforts associated with administering web-based access to multiple systems, but simultaneously introduces additional risks in that an incorrect assignment of access may result in inappropriate access to multiple systems.
- *Data content quality* - As enterprise applications are opened to external suppliers and customers, the need for integrity in enterprise data becomes paramount.
- *Privacy and confidentiality* - Regularity and governance issues surrounding the increased capture and visibility of personal information, i.e. spending habits.

(b) While performing an IS audit, auditors should ascertain that the following objectives are met:

- (i) Security provisions protect computer equipments, programs, communications and data from unauthorized access, modification, or destructions.
- (ii) Program development and acquisition is performed in accordance with management's general and specific authorization.
- (iii) Program modifications have the authorization and approval of management.
- (iv) Processing of transactions, files, reports and other computer records is accurate and complete.
- (v) Source data that is inaccurate or improperly authorized is identified and controlled according to prescribed managerial policies.
- (vi) Computer data files are accurate, complete and confidential.

(c) Chapter-II, Section 3 of Information Technology (Amendment) Act 2008 provides conditions subject to which an electronic record is authenticated by means of affixing digital signature.

- The digital signature is created in two distinct steps. First the electronic record is converted into a message digest by using a mathematical function known as "hash function" which digitally freezes the electronic record thus ensuring the integrity of the content of the intended communication contained in the electronic record.

Any tampering with the contents of the electronic record will immediately invalidate the digital signature.

- Secondly, the identity of the person affixing the digital signature is authenticated through the use of a private key which attaches itself to the message digest and which can be verified by anybody who has the

corresponding public key.

This will enable anybody to verify whether the electronic record is retained intact or has been tampered with; since it was fixed with the digital signature. It will also enable a person who has a public key to identify the originator of the message.

3. (a) Pre-requisites of an MIS: The following are main pre-requisites of an effective MIS:

- (i) **Database:** It is a super file, which consolidates data records formerly stored in many data files. The data in database is organized in such a way that access to the data is improved and redundancy is reduced. Normally, the database is subdivided into major information sub-sets needed to run. The database should be user-oriented, capable of being used as a common data source, available to authorized persons only and should be controlled by a separate authority such as DBMS. Such a database is capable of meeting information requirements of its executives, which is necessary for planning, organizing and controlling the operations of the business.
- (ii) **Qualified System and Management Staff:** MIS should be manned by qualified officers. These officers who are experts in the field should understand clearly the views of their fellow officers. The organizational management base should comprise of two categories of officers (i) System and Computer experts and (ii) Management experts. Management experts should clearly understand the concepts and operations of a computer. Their whole hearted support and cooperation will help in making MIS an effective one.
- (iii) **Support of Top Management:** An MIS becomes effective only if it receives the full support of top management. To gain the support of top management, the officer should place before them all the supporting facts and state clearly the benefits which will accrue from it to the concern. This step will certainly enlighten the management and will change their attitude towards MIS.
- (iv) **Control and Maintenance of MIS:** Control of the MIS means the operation of the system as it was designed to operate. Sometimes users develop their own procedures or shortcut methods to use the system, which reduces its effectiveness. To check such habits of users, the management at each level in the organization should device checks for the information system control.

Maintenance is closely related to control. There are times when the need for improvements to the system will be discovered. Formal methods for changing and documenting changes must be provided.
- (v) **Evaluation of MIS:** An effective MIS should be capable of meeting the information requirements of its executives in future as well. The capability can be maintained by evaluating the MIS and taking appropriate timely action. The evaluation of MIS should take into account the following points:

Examining the flexibility to cope with future requirements;

Ascertaining the view of the users and designers about the capabilities and deficiencies of the system ; and

Guiding the appropriate authority about the steps to be taken to maintain effectiveness of MIS.

- (b) **Physical and Environmental Security:** This is the beginning point of any security plan. It is designed to prevent unauthorized access, damage and interference to business premises and information. This involves physical security perimeter, physical entry control, creating secure offices, rooms, facilities, providing physical access controls, providing protection devices to minimize risks ranging from fire to electromagnetic radiation, providing adequate protection to power supplies and data cables. Cost effective design and constant monitoring are two key aspects to maintain adequate physical security control.

Maintenance of the physical operating environment in a computer server room is as important as ensuring that paper records are not subject to damage by mould, fire or fading. Supporting equipments such as air conditioning plant etc. should be properly maintained. Physical controls may be difficult to manage as they rely to some extent on building structure, but good physical security can be very effective.

The detailed **controls and objectives** for this type of security are:

- *Secure areas:* To prevent unauthorized access, damage and interference to business premises and information,
 - *Equipment Security:* To prevent loss, damage or compromise of assets and interruption to business activities, and
 - *General Controls:* To prevent compromise or theft of information and information processing facilities.
- (c) To some extent, systems analysis and development has been greatly improved by the introduction of prototyping. Prototyping enables the user to take an active part in the systems design, with the analyst acting in an advisory role.

Prototyping makes use of the expertise of both the user and the analyst, thus ensuring better analysis and design, and prototyping is a crucial tool in that process.

Other advantages of prototyping include:

- improving the fact finding process;
- improving relations between analysts and users;
- encouraging the users to 'own' the new system;
- reducing the cost of user training;
- identification of system problems; and

- ensuring quality for the eventual system.

4. (a) The term disaster can be defined as an incident, which jeopardizes business operations and/or human life. It could be due to sabotage (human) or natural. Following is the procedural plans for disaster recovery.

Disaster Recovery Procedural Plan: Normally disaster recovery procedural plan is made when the system is normally working. After visualizing the disaster the action to be taken by different people of the organization are to be documented. This recovery and planning document may include the following areas:

- (i) The conditions for activating the plans, which describe the process to be followed before each plan, are activated.
- (ii) Emergency procedures, which describe the actions to be taken following an incident which jeopardizes business operations and/or human life. This should include arrangements for public relations management and for effective liaison with appropriate public authorities e.g. police, fire, services and local government.
- (iii) Fallback procedures which describe the actions to be taken to move essential business activities or support services to alternate temporary locations, to bring business process back into operation in the required time-scale.
- (iv) Resumption procedures, which describe the actions to be taken to return to normal business operations.
- (v) A maintenance schedule, which specifies how and when the plan will be tested, and the process for maintaining the plan.
- (vi) Awareness and education activities, which are designed to create an understanding of the business continuity, process and ensure that the business continues to be effective.
- (vii) The responsibilities of individuals describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.
- (viii) Contingency plan document distribution list.
- (ix) Detailed description of the purpose and scope of the plan.
- (x) Contingency plan testing and recovery procedure.
- (xi) List of vendors doing business with the organization, their contact numbers and address for emergency purposes.
- (xii) Checklist for inventory taking and updating the contingency plan on a regular basis.
- (xiii) List of phone numbers of employees in the event of an emergency.
- (xiv) Emergency phone list for fire, police, hardware, software, suppliers,

customers, back-up location, etc.

- (xv) Medical procedure to be followed in case of injury.
- (xvi) Back-up location contractual agreement, correspondences.
- (xvii) Insurance papers and claim forms.
- (xviii) Primary computer centre hardware, software, peripheral equipment and software configuration.
- (xix) Location of data and program files, data dictionary, documentation manuals, source and object codes and back-up media.
- (xx) Alternate manual procedures to be followed such as preparation of invoices.
- (xxi) Names of employees trained for emergency situation, first aid and life saving techniques.
- (xxii) Details of airlines, hotels and transport arrangements.

(b) A good security policy should clearly state the following:

- Purpose and scope of the document and the intended audience;
- The security infrastructure;
- Security policy document maintenance and compliance requirements;
- Incident response mechanism and incident reporting;
- Security organization structure;
- Inventory and classification of assets;
- Description of technologies and computing structure;
- Physical and environmental security;
- Identify management and access control;
- IT operations management;
- IT communications;
- System development and maintenance controls;
- Business continuity planning;
- Legal compliances;
- Monitoring and Auditing Requirements; and
- Underlying technical policy.

(c) The challenges involved in ERP implementation are:

- (i) Consultants, vendors and users have to work together to achieve the overall

objectives of the organization. The consultants have to clearly understand the user needs and the prevailing business realities and design the business solutions keeping in mind all these factors.

- (ii) Proper customization of package to the organization has to be in tune with the users needs and business objectives.
- (iii) Roles and responsibilities of the employees have to be clearly identified, understood and configured in the system.
- (iv) Acceptance by employees for the new processes and procedures is critical for the success of the package.
- (v) Package to be implemented in totality to achieve the maximum benefit.
- (vi) Defining the implementation methodology to be followed – identifying needs, evaluation of the current situation, predicting the future situation, reengineering the business process, selection of correct package.
- (vii) Installation of hardware, software required for the package.
- (viii) Selection of right kind of consultants.
- (ix) Preparing the implementation guidelines – training users, effective leadership, adapting the new systems and making changes in the working environment etc.
- (x) Post implementation monitoring of Key Performance indicators, Critical success factors etc.

5. (a) **Information:** Information is data that have been put into a meaningful and useful context. It has been defined by Davis and Olson as-“information is data that has been processed into a form that is meaningful to the recipient and is of real or perceived value in current or progressive decision”. For example, data regarding sales by various salesmen can be merged to provide information regarding total sales through sales personnel. This information is of vital importance to a marketing manager who is trying to plan for future sales.

Attributes of Information: The important attributes of useful and effective information are as follows:

- **Availability:** This is a very important property of information. If information is not available at the time of need, it is useless. Data is organized in the form of facts and figures in databases and files from where various information is derived for useful purpose.
- **Purpose:** Information must have purposes at the time it is transmitted to a person or machine, otherwise it is simple data. Information communicated to people has a variety of purposes because of the variety of activities performed

by them in business organizations. The basic purpose of information is to inform, evaluate, persuade, and organize.

- **Mode and format:** The modes of communicating information to humans are sensory (through sight, hear, taste, touch and smell) but in business they are either visual, verbal or in written form.

Format of information should be so designed that it assists in decision making, solving problems, initiating planning, controlling and searching. Therefore, all the statistical rules of compiling statistical tables and presenting information by means of diagram, graphs, curves, etc., should be considered and appropriate one followed. The reports should preferably be supplied on an exception basis to save the manager from an overload of information. Also, the data should only be classified into those categories, which have relevance to the problem at hand.

- **Decay:** Value of information usually decays with time and usage and so it should be refreshed from time to time. From example, we access the running score sheet of a cricket match through Internet sites and this score sheet is continually refreshed at a fixed interval or based on status of the state. Similarly, in highly fluctuating share market a broker is always interested about the latest information of a particular stock/s.
- **Rate:** The rate of transmission/reception of information may be represented by the time required to understand a particular situation. Quantitatively, the rate for humans may be measure by the number of numeric characters transmitted per minute, such as sales reports from a district office. For machines the rate may be based on the number of bits of information per character (sign) per unit of time.
- **Frequency:** The frequency with which information is transmitted or received affects its value. Financial reports prepared weekly may show so little changes that they have small value, whereas monthly reports may indicate changes big enough to show problems or trends.

Frequency has some relationship with the level of management also it should be related to an operational need. For example, at the level of foreman it should be on a daily or weekly basis but, at the management control level, it is usually on monthly basis.

- **Completeness:** The information should be as complete as possible. The classical ROI or Net Present Value (NPV) models just provide a point estimate and do not give any indication of the range within which these estimates may vary. Hartz's model for investment decisions provides information on mean, standard deviation and the shape of the distribution of ROI and NPV. With this

complete information, the manager is in a much better position to decide whether or not to undertake the venture.

- **Reliability:** It is just not authenticity or correctness of information; rather technically it is a measure of failure or success of using information for decision-making. If information leads to correct decision on many occasions, we say the information is reliable.
 - **Cost benefit analysis:** The benefits that are derived from the information must justify the cost incurred in procuring information. The cost factor is not difficult to establish. Using costing techniques, we shall have to find out the total as well as the marginal cost of each managerial statement but benefits are hard to quantify, i.e., they are usually intangibles. In fact, the assessment of such benefits is very subjective and its conversion into objective units of measurement is almost impossible. However, to resolve this problem, we can classify all the managerial statements into many categories with reference to the degree of importance.
 - **Validity:** It measures the closeness of the information to the purpose which it purports to serve. For example, some productivity measure may not measure, for the given situation, what they are supposed to do e.g., the real rise or fall in productivity. The measure suiting the organization may have to be carefully selected or evolved.
 - **Quality:** Quality refers to the correctness of information. Information is likely to be spoiled by personal bias. For example, an over-optimistic salesman may give rather too high estimates of the sales. This problem, however, can be circumvented by maintaining records of salesman's estimates and actual sales and deflating or inflating the estimates in the light of this.
 - **Transparency:** If information does not reveal directly what we want to know for decision-making, it is not transparent. For example, total amount of advance does not give true picture of utilization of fund for decision about future course of action; rather deposit-advance ratio is perhaps more transparent information in this matter.
- (b) Important factors to assist the auditors in making related determination are given as follows:
- (i) The extent to which internal controls that are significant to the audit depend on the reliability of information processed or generated by information systems.
 - (ii) The availability of evidence outside the information system to support the findings and conclusions: It may not be possible for auditors to obtain sufficient, appropriate evidence without assessing the effectiveness of relevant information systems controls. For example, if information supporting the findings and conclusions is generated by information systems or its reliability is

dependent on information systems controls; there may not be sufficient supporting or corroborating information or documentary evidence that is available other than that produced by the information systems.

- (iii) The relationship of information systems controls to data reliability: To obtain evidence about the reliability of computer generated information, auditors may decide to assess the effectiveness of information systems controls as part of obtaining evidence about the reliability of the data. If the auditor concludes that information systems controls are effective, the auditor may reduce the extent of direct testing of data.
 - (iv) Assessing the effectiveness of information systems controls as an audit objective: When assessing the effectiveness of information systems controls is directly a part of audit objective, auditors should test information systems controls necessary to address the audit objectives. For example, the audit may involve the effectiveness of information systems controls related to certain systems, facilities, or organizations.
- (c) Information developed in the testing phase that an auditor should document includes the following:
- An understanding of the information systems that are relevant to the audit objectives
 - IS Control objectives and activities relevant to the audit objectives
 - By level (e.g., entitywide, system, business process application) and system sublevel e.g., network, operating system, infrastructure applications), a description of control techniques used by the entity to achieve the relevant IS control objectives and activities.
 - By level and sublevel, specific tests performed, including:
 - Ø related documentation that describes the nature, timing, and extent of the tests;
 - Ø evidence of the effective operation of the control techniques or lack thereof (e.g., memos describing procedures and results, output of tools and related analysis);
 - Ø if a control is not achieved, any compensating controls or other factors and the basis for determining whether they are effective;
 - Ø the auditor's conclusions about the effectiveness of the entity's IS controls in achieving the control objective; and
 - Ø for each weakness, whether the weakness is a material weakness, significant deficiency or just a deficiency, as well as the criteria, condition, cause, and effect if necessary to achieve the audit objectives.

6. (a) Following are some of the reasons due to which the organizations fail to achieve their system development objectives:
- (i) **Lack of senior management support for and involvement in information system development:** In the management of information systems, developers and users depend on the senior management for support and to determine which systems development projects are important. Their tendency is to shift away from the project, which lack senior management attention.
 - (ii) **Shifting user needs:** User requirements for information technology are constantly varying. 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.
 - (iii) **Development of strategic systems:** 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.
 - (iv) **New technologies:** New technologies are coming in the organizations want to apply these and create a competitive situation. However, later they find that attaining systems development objectives is more difficult because personnel are not familiar with the new technology.
 - (v) **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 the budget.
 - (vi) **Overworked or under-trained development staff:** It is generally established that there is backlog of systems development work due to lack of efficient staff. In addition to being overworked, system developers often lack sufficient educational background. Many companies do little to help their development personnel stay technically updated and in these organizations, a training plan and training budget do not exist.
 - (vii) **Resistance to change:** People have a natural tendency to resist change, and information systems development projects signal changes –often radical – in the work place. 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 will dig in their heels, and the development project is doomed to failure. Personnel cutbacks often result when reengineering projects really attempt at downsizing (or right sizing).
 - (viii) **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.

- (ix) **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. By executing the system development process efficiently and effectively, the above problem can be solved.
- (b) **Types of system's Back-ups:** When the back-ups are taken of the system and data together, they are called total system's back-up. System back-up may be a full back-up, an incremental back-up or a differential back-up.
 - (i) *Full Backup:* Every backup generation contains every file in the backup set. However, the amount of time and space such a backup takes prevents it from being a realistic proposition for backing up a large amount of data. This is the simplest form of backup with a single restoring session for restoring all backed-up files.
 - (ii) *Differential Backup:* It contains all the files that have changed since the last full backup. This is in contrast to incremental backup generation, which holds all the files that were modified since the last full or incremental backup. It is faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved.
 - (iii) *Incremental Backup:* Only the files that have changed since the last full backup / differential backup / or incremental backup are saved. This is the most economical method, as only the files that changed since the last backup are backed up. This saves a lot of backup time and space. Normally, it is difficult to restore as you have to start with recovering the last full backup, and then recovering from every incremental backup taken since.
 - (iv) *Mirror back-up:* It is identical to a full backup, with the exception that the files are not compressed in zip files and they can not be protected with a password. A mirror backup is most frequently used to create an exact copy of the backup data.

- (c) **Types of Information Protection:** Two basic types of information protection that an organization can use are given as follows:

1. Preventative Information Protection, and
2. Restorative Information Protection.

Preventative Information Protection: It is based on use of security controls, which itself is a group of three types of controls such as Physical, Logical, and Administrative.

- *Physical controls* deal with Doors, Locks, Guards, Floppy Disk Access Locks, Cables locking systems to desks/walls, CCTV, Paper Shredders, Fire Suppression Systems,
- *Logical controls* deal with Passwords, File Permissions, Access Control Lists, Account Privileges, Power Protection Systems, and
- *Administrative controls* deal with Security Awareness, User Account Revocation, and Policy.

Restorative Information Protection: If an organization cannot recover or recreate critical information systems in an acceptable time period, the organization will suffer and possibly have to go out of business. Hence, the key requirement of any restorative information system protection plan is that the information systems can be recovered. The claim of back program to backup data automatically cannot be reliable. It has so many problems. The restorative information protection program must address the following:

- Whether the recovery process has been evaluated and tested recently?
- The time taken for restoration,
- The quantum of productivity loss,
- The strict adherence of plan, and
- The time needed to input the data changes since the last backup.

7. (a) **CASE Tools :** The data flow diagram and system flow charts that users review are commonly generated by systems developers using the on-screen drawing modules found in **CASE** (Computer-Aided-Software Engineering) software packages. CASE refers to the automation of anything that humans do to develop systems and support virtually all phases of traditional system development process. For example, these packages can be used to create complete and internally consistent requirements specifications with graphic generators and specifications languages.

An ideal CASE system would have an integrated set of tools and features to perform all aspects in the life cycle. Some of the features that various CASE products possess are - Repository / Data Dictionary; Computer aided Diagramming Tools; Word Processing; Screen and Report generator; Prototyping; Project Management; Code Generation; and Reverse Engineering.

- (b) **Data Dictionary:** A data dictionary is a computer file that contains descriptive information about the data items in the files of a business information system. Thus, a data dictionary is a computer file about data. Each computer record of a data dictionary contains information about a single data item used in a business information system. This information may include:

- Codes describing the data item's length (in characters), data type (alphabetic, numeric, alphanumeric, etc.), and range (e.g., values from 1 to 99 for a department code)
 - The identity of the source document(s) used to create the data item.
 - The names of the computer files that store the data item.
 - The names of the computer programs that modify the data item.
 - The identity of the computer programs or individuals permitted to access the data item for the purpose of file maintenance, upkeep, or inquiry.
 - The identity of the computer programs or individuals not permitted to access the data item.
- (c) **Technical Feasibility:** It is concerned with hardware and software. Essentially, the analyst ascertains whether the proposed system is feasible with existing or expected computer hardware and software technology. The technical issues usually raised during the feasibility stage of investigation include the following:
- Does the necessary technology exist to do what is suggested (and can it be acquired)?
 - Does the proposed equipment have the technical capacity to hold the data required to use the new system?
 - Will the proposed system provide adequate responses to inquiries, regardless of the number or location of users?
 - Can the system be expanded if developed?
 - Are there technical guarantees of accuracy, reliability, ease of access, and data security?
- (d) **Firewall:** A firewall is a collection of components (computers, routers, and software) that mediate access between different security domains. All traffic between the security domains must pass through the firewall, regardless of the direction of the flow. Since the firewall serves as an access control point for traffic between security domains, they are ideally situated to inspect and block traffic and coordinate activities with network intrusion detection system (IDSs).

There are four primary firewall types from which to choose: packet filtering, stateful inspection, proxy servers, and application-level firewalls. Any product may have characteristics of one or more firewall types. The selection of firewall type is dependent on many characteristics of the security zone, such as the amount of traffic, the sensitivity of the systems and data, and applications. Additionally, consideration should be given to the ease of firewall administration, degree of firewall monitoring support through automated logging and log analysis, and the capability to provide alerts for abnormal activity.

Typically, firewalls block or allow traffic based on rules configured by the administrator. Rule sets can be static or dynamic. A static rule set is an unchanging statement to be applied to packet header, such as blocking all incoming traffic with certain source addresses. A dynamic rule set often is the result of coordinating a firewall and an IDS. For example, an IDS that alerts on malicious activity may send a message to the firewall to block the incoming IP address. The firewall, after ensuring that the IP is not on a "white list", creates a rule to block the IP. After a specified period of time the rule expires and traffic is once again allowed from that IP.

Firewalls are subject to failure. When firewalls fail, they typically should fail closed, blocking all traffic, rather than failing open and allowing all traffic to pass. Firewalls provide some additional services such as network address translation, dynamic host configuration protocols and virtual private network gateways.

- (e) **Hacking:** It is an act of penetrating computer systems to gain knowledge about the system and how it works. Technically, a hacker is someone who is enthusiastic about computer programming and all things relating to the technical workings of a computer.

Crackers are people who try to gain unauthorized access to computers. This is normally done through the use of a "backdoor" program installed on the machine. A lot of crackers also try to gain access to resources through the use of password cracking software, which tries billions of passwords to find the correct one for accessing a computer.

There are many ways in which a hacker can hack. These are:

- Net BIOS,
- ICMP Ping,
- FTP,
- RPC. Statd, and
- HTTP.