- Organizational Costs of data loss
- Incorrect decision making
- Cost of Computer Abuse
- Value of Computer Hardware, Software and Personnel
- High cost of Computer Error
- Maintenance of Privacy
- Controlled evolution of computer use
- Definition Information System Audit
- Objectives – Asset safeguarding, Data Integrity, System Effectiveness, System efficiency.

- **Organizational Costs of data loss:**
  - ✓ Data is a critical resource of an organization for its present and future process and its ability to adapt and survive in a changing environment.
  - ✓ Data provides the organization with an image of itself its environment, its history and its future.
  - ✓ If the data is inaccurate or lost, the organization can incur substantial losses.
  - ✓ There should be proper backup of computer files.
- **Incorrect decision making:**
  - ✓ Management and operational controls taken by managers involve detection, investigations and correction of out-of-control processes. These high level decisions require accurate data to make quality decision rules.
  - ✓ Decision making depends on the data and quantity of decision rules that exists in the computer-based information system.
  - ✓ Inaccurate data causes costly, unnecessary investigations and out of control process can also remain undetected.
- **Cost of Computer Abuse:**
  - ✓ *Hacking:* A person gaining unauthorized access of system to modify or delete program or to disrupt services.
  - ✓ *Viruses:* It is a program that attaches itself to executable files or data files and replicate themselves and cause disruption.
  - ✓ *Illegal Physical Access:* A person gaining unauthorized physical access in the system, can cause physical damage or make copies of data.
  - ✓ *Abuse of privileges:* A person uses privileges for unauthorized purposes, making copies of sensitive data they are permitted to access.
  - ✓ Unauthorized access to computer systems, computer viruses, unauthorized physical access to computer facilities and unauthorized copies of sensitive data can lead to destruction of assets (hardware, software, documentation etc.)
- **Value of Computer Hardware, Software and Personnel:**

- ✓ These are critical resources of an organization which has a credible impact on its infrastructure and business competitiveness.
- ✓ In addition to data hardware and software are critical organizational resources.
- ✓ Some intentional or unintentional loss of hardware can cause disruption in functioning of organization.
- ✓ If the software is corrupted the confidential information could be stolen could be disclosed to competitors.

High cost of Computer Error:

- ✓ In a computerized enterprise environment where many critical business processes are performed a data error during entry or process would cause great damage.
- ✓ Computers automatically perform many critical functions, such as ATM services, online banking and accurate tracking and verification of funds.

Maintenance of Privacy:

- ✓ Today data collected in a business process contains details about an individual on medical, educational, employment, residence etc. These data were also collected before computers but now there is a fear that privacy has eroded beyond acceptable levels.
- ✓ All the important data of an individual like financial information, personal data everything is stored on computers.
- ✓ If there is some breach in the system, all the private data will be gone in seconds thus making it important to protect and maintain the privacy.

Controlled evolution of computer use:

- ✓ Technology use and reliability of complex computer systems cannot be guaranteed and the consequences of using unreliable systems can be destructive.

Definition Information System Audit:

- ✓ Auditing is the process of assessment of financial, operational, strategic goals and processes in organizations to determine whether they are in compliance with the stated principles, regulatory norms, rules and regulations.
- ✓ It is the process of attesting objectives (those of the external auditor) that focus on asset safeguarding and data integrity, and management objectives (those of the internal auditor) that include not only attest objectives but also effectiveness and efficiency objectives.
- ✓ Aim of IS audit is to safeguard the assets, to maintain data integrity, to achieve system effectiveness and to achieve system efficiency.
- ✓ The audit can be conducted internally by employees of the organization or externally by an outside firm.

Objectives – Asset safeguarding, Data Integrity, System Effectiveness, System efficiency:

- ✓ **Asset Safeguarding Objectives:**
  - The IS assets includes Hardware, Software, People, Data files and System documentation.

- These assets play a major role in organizational growth. Thus, making it necessary to safeguard these assets.
- So, the assets must be protected by a system of internal controls from unauthorized access.

✓ **Data Integrity Objectives:**

- Data integrity is a fundamental concept of IS auditing.
- It is a state implying that data has certain attributes, like: Completeness, Soundness, Purity and Veracity.
- The importance to maintain integrity of data of an organization depends on the value of information, the extent of access to the information and the value of data to the business from the perspective of the decision maker, competition and the market environment.
- If the integrity of an organization's data is low it could suffer a great loss.

✓ **System Effectiveness Objectives:**

- The effectiveness is the measure for deciding whether the system provides the desired output or not. Being effective means producing the right output in terms of quantity and quality.
- Effectiveness auditing is done usually after the system has been running for some time.
- It can be carried out during the design stages of system.

✓ **System Efficiency Objectives:**

- The efficiency indicates the manner in which the inputs are used by the system. Being efficient means the system uses in a "right way".
- An efficient IS uses minimum resources to achieve its required objectives.
- To optimize the use of various information system resources (machine time, peripherals, system software and labour) along with the impact on its computing environment.

* * * * *