1) Explain in detail about critical characteristics of information. (Nov/Dec 2011, May/June 2012, Nov/Dec 2012, May/June 2014)

Availability

- Availability enables users who need to access information to do so without interference or obstruction, and to receive it in the required format.
- Availability of information
  - ✔ Is accessible to any user.
  - ✔ Requires the verification of the user as one with authorized access to the information.
- The information, then, is said to be available to an authorized user when and where needed and in the correct format.

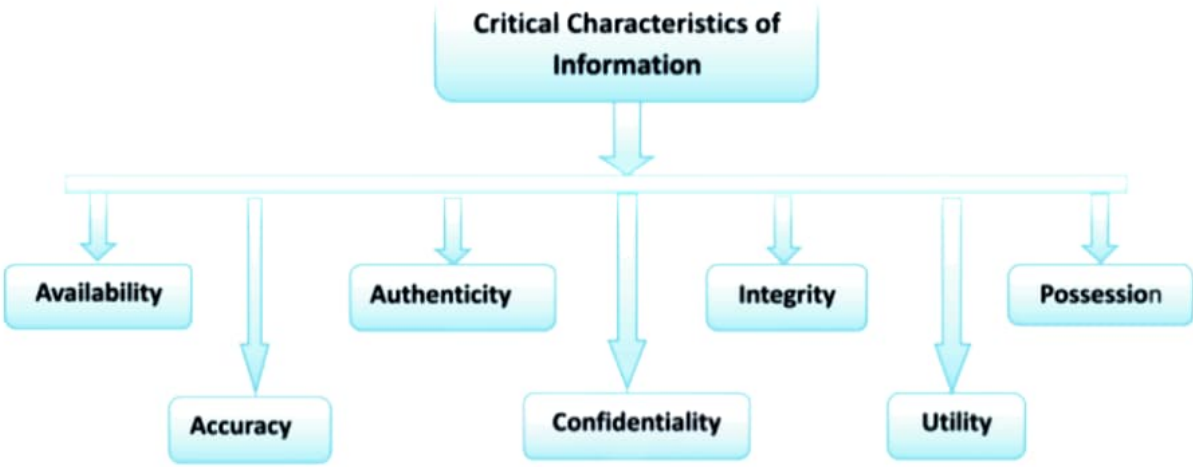

Fig: Critical Characteristics of Information

Example:-

Consider the contents of a library

- Research libraries that require identification before entrance.
- Librarians protect the contents of the library, so that it is available only to authorized patrons.
- The librarian must see and accept a patron's proof of identification before that patron has free and easy access to the contents available in the bookroom.

Accuracy

Information is accurate

- ✔ when it is free from mistakes or errors and
- ✔ It has the value that the end user expects.

Information contains a value different from the user's expectations due to the intentional or unintentional modification of its content, it is no longer accurate.

Example:-

Consider the checking account

- Inaccuracy of the information in your checking account can be caused by external or internal means.
- If a bank teller, for instance, mistakenly adds or subtracts too much from your account, the value of the information has changed.
- In turn, as the user of your bank account, you can also accidentally enter an incorrect amount into your account register. This also changes the value of the information.

Authenticity

- Authenticity of information is the quality or state of being genuine or original, rather than a reproduction or fabrication.
- Information is authentic when it is the information that was originally
  - ✔ Created,

- ✔ Placed,
- ✔ Stored, or
- ✔ Transferred.

Example:-

Consider for a moment some of the assumptions made about e-mail.

- ✔ When you receive e-mail, you assume that a specific individual or group of individuals created and transmitted the e-mail—you assume know the origin of the e-mail. This is not always the case.
- ✔ E-Mail spoofing, the process of sending an e-mail message with a modified field, is a problem for many individuals today, because many times the field modified is the address of the originator.
- ✔ Spoofing the address of origin can fool the e-mail recipient into thinking that the message is legitimate traffic.
- ✔ In this way, the spoofed can induce the e-mail readers into opening e-mail they otherwise might not have opened.
- ✔ The attack known as spoofing can also be applied to the transmission of data across a network, as in the case of user data protocol (UDP) packet spoofing, which can enable unauthorized access to data stored on computing systems.

Confidentiality

- The confidentiality of information is the quality or state of preventing disclosure or exposure to unauthorized individuals or systems.
- Confidentiality of information is ensuring that only those with the rights and privileges to access a particular set of information are able to do so, and that those who are not authorized are prevented from obtaining access.
- When unauthorized individuals or systems can view information, confidentiality is breached.
- To protect the confidentiality of information, you can use a number of measure:
  - ✔ Information classification
  - ✔ Secure documents storage
  - ✔ Application of general security policies
  - ✔ Education of information custodians and end users

Example:-

Ex: 1 A security is an employee throwing away a document containing critical information without shredding it.

Ex: 2 A hacker who successfully breaks into an internal database of a Web-based organization and steals sensitive information about the clients such as

- ✔ Names
- ✔ Addresses and
- ✔ Credit card numbers.

Integrity

- The quality or state of being whole, complete, and uncorrupted is the integrity of information.
- The integrity of information is threatened when the information is exposed to
  - ✔ Corruption,
  - ✔ Damage,
  - ✔ Destruction, or
  - ✔ Other disruption of its authentic state.
- The threat of corruption can occur while information is being stored or transmitted.
- Many computer viruses and worms have been created with the specific purpose of corrupting data.

For this reason the key method for detecting the virus or worm

1. First Key methodology is to look for changes in file integrity as shown by the size of the file.
2. Another key methodology for assuring information integrity is through file hashing.
   - ✔ With file hashing, a file is read by a special algorithm that uses the value of the bits in the file to compute a single large number called a Hash value.
   - ✔ The hash value for any combination of bits is different for each combination.

Utility

- The Utility information is the quality or state of having value for some purpose or end.
- Information has value when it serves a particular purpose. This means that if information is available, but not in a format meaningful to the end user, it is not useful.

Possession

- The Possession of information is the quality or state of having ownership or control of some object or item.
- Information is said to be in possession if one obtains it, independent of format or other characteristic.
- A breach of confidentiality always results in a breach of possession, a breach of possession does not always result in a breach of confidentiality.

Example:-

- ✔ Assume a company stores its critical customer data using an encrypted file system.
- ✔ An employee, who has quit, decides to take a copy of the tape backups to sell the customer records to the competition.
- ✔ The removal of the tapes from their secure environment is a breach of possession, because the data is encrypted, neither the employee nor anyone else can read it without the proper decryption methods, therefore there is no breach of confidentiality.