Types of Controls

Implementation of controls is a critical security feature of information systems. They block and detect various forms of intrusion and protect various components of the entire information systems, are these telecommunication lines or computer software's and hard wares.

1. **Access Controls** – Controlling who can access the system.
2. **Input Controls** – Controls over how the data is input to the system.
3. **Communication Controls** – Controls over the transfer of data between LAN, WAN or internet.
4. **Processing Controls** – controlling the processing of data
5. **Database Controls** – Securing the most important asset of the organization
6. **Output controls** – controlling the privacy of the data.

34.1 Access Controls

These controls establish the interface between the would-be user of the computer system and the computer itself. These controls monitor the initial handshaking procedure of the user with the operating system. For example when a customer enter the card and the pin code in an automatic teller machine (ATM), the access controls are exercised by the system to block unwanted or illegitimate access.

The identity of the user needs to be established before granting access. The user should be given access to the nature and kind of resources he is entitled to access. Actions taken by users to have access beyond the limits defined should be blocked and recorded.

Why Access Controls?

Access controls have gained critical importance in the modern computing age for two significant reasons.

- Widespread deployment of distributed systems has resulted in many users being disbursed physically. e.g. through Web based systems, local Area Networks, wide Area Networks
- The rapid growth of E-Commerce systems has resulted in substantial work being undertaken to identify and authenticate the parties.

Cryptography means science of coded writing. It is a security safeguard to render information unintelligible if unauthorized individuals intercept the transmission. When the information is to be used, it can be decoded. "The conversion of data into a secret code for the secure transmission over a public network is called cryptography."

Encryption & Decryption

Cryptography primarily consists of two basic processes. These processes are explained through diagram.

Encryption – the process of converting data into codes (cryptograms)

- Decryption – the process of decoding the code arrived at data actually encrypted

The above processes give rise to two forms of data

- Clear text – it is the data to be encrypted.
- Cipher text – it is the code created out of data after encryption

As shown in the above diagram, the original text, or "plaintext," is converted into a coded equivalent called "ciphertext" via an encryption process.

Identification & Authentication

Access controls focus on the correct identification of the user seeking permission to access the system. There can be various sources of identifying and authenticating the user.

1. What a user remembers – name, birthdate, password
2. What a user possesses – badge, plastic card
3. What a user is – personal characterictics

In addition to the aforesaid access controls, there may be

1. Input controls – controls over correct data entry

2. Communications controls – controls over transporting data safely through local area networks (LAN's) or wide area networks (WAN's).

3. Processing controls – Controls over the integrity of processing instructions being executed by the operating system and application software's.

4. Database controls – implemented to maintain the integrity of the database.

5. Output controls – controls over providing right content to the users.

The construction of effective security system should take into account the design and implementation of all the above controls.

Processing instructions carried out by the operating system and application software should be monitored by implementation of controls. If the processing controls are not effectively implemented, we could have undesirable situations arising. For example, in case of an operating system, while connecting to a website, a concealed link may be activated at the same time to transfer specified or all information. In case of an application software designed to compute interest at month end may contain unauthorized instruction to transfer pennies or cents or paisas to a particular account. Hence care needs to be taken that calculations are accurate and any rounding up or down is adequately explained and carried out, data is processed correctly as expected, control totals reconcile and processing errors are logged, researched and corrected timely and sufficient audit trail to trace from source to output and vice versa.