**CNSS**

**committee On Network Security System has a 3 dimentional security model which has becoma a standard model for many of operating information sysytem.**

**Information Security programs are build around 3 objectives, commonly known as CIA –** Confidentiality, Integrity, Availability.   
**Key Of Goal.**

1. **Confidentiality –** means information is not disclosed to unauthorized individuals, entities and process. For example if we say I have a password for my Gmail account but someone saw while I was doing a login into Gmail account. In that case my password has been compromised and Confidentiality has been breached.
2. **Integrity –** means maintaining accuracy and completeness of data. This means data cannot be edited in an unauthorized way. For example if an employee leaves an organisation then in that case data for that employee in all departments like accounts, should be updated to reflect status to JOB LEFT so that data is complete and accurate and in addition to this only authorized person should be allowed to edit employee data.
3. **Availability –** means information must be available when needed. For example if one needs to access information of a particular employee to check whether employee has outstanded the number of leaves, in that case it requires collaboration from different organizational teams like network operations, development operations, incident response and policy/change management.   
   Denial of service attack is one of the factor that can hamper the availability of information.

**Three information States .**

* Transmision.
* Storage .
* Processing.

**Model has three Measure Security.**

* Educational awareness
* Technologies
* Polices and practices

**Profetions and Organization :**

* **Governance :**

The board of directors coming together to make a decision about the direction of the company

Their duties Such as Planing ,Decision making and financial planning.

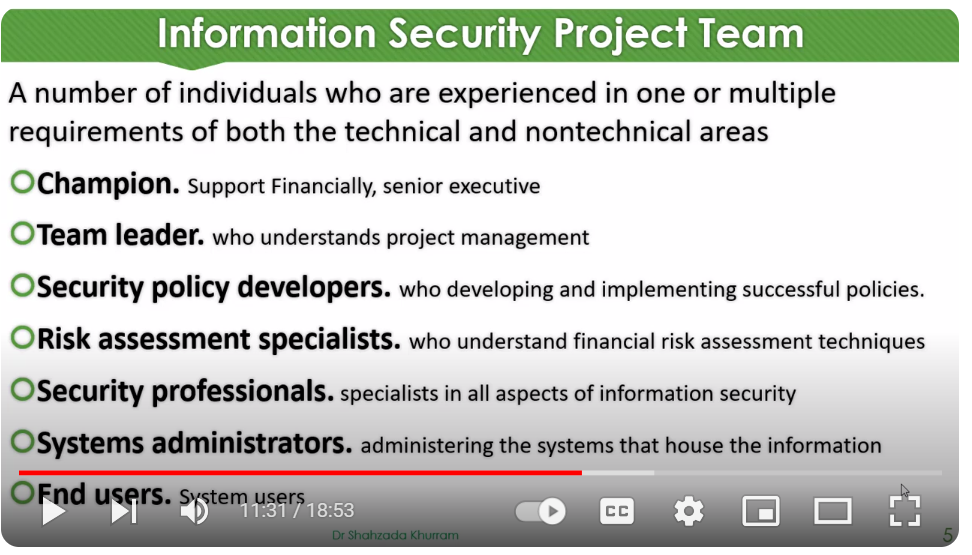
Risk apititute, agresion and neutral advicer.

* **Management:**

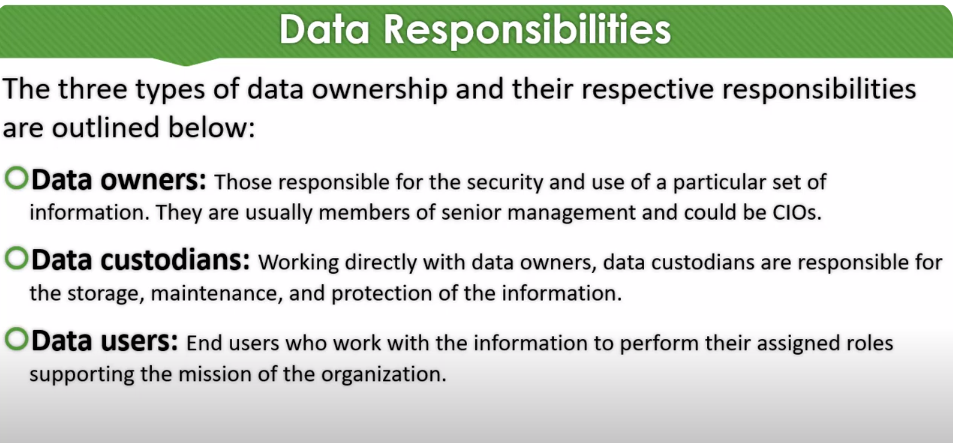
the management Runs the palns theat is set by the governance .

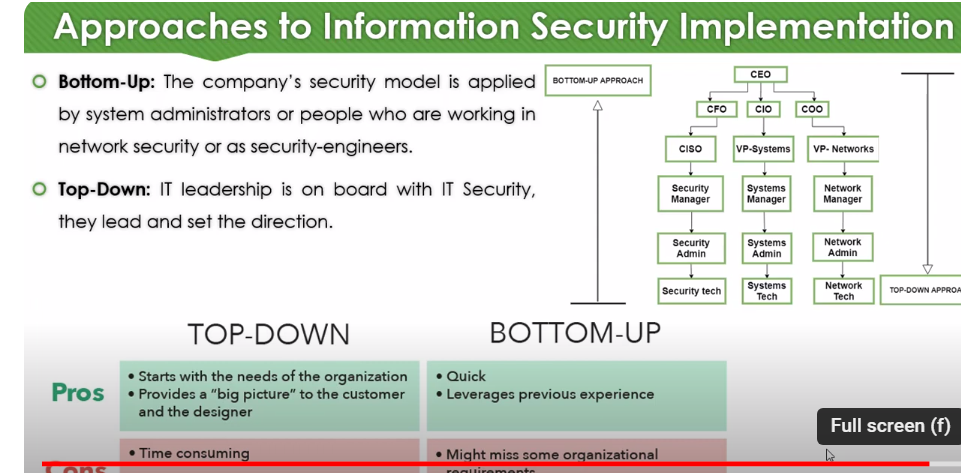
The management analysis the risk and Practically work their risk and envoirnment.

**Information Security Project Team**



**Data Responsibilities’**





**Types of encryption;**

Symmetric encryption is the use of a single secret key to exchange information. Because it

uses one key for encryption and decryption, the sender and receiver must know the secret

key to lock or unlock the cipher.

**Symmetric algorithms;**

** Triple DES (3DES)** is known as a block cipher because of the way it converts plaintext into

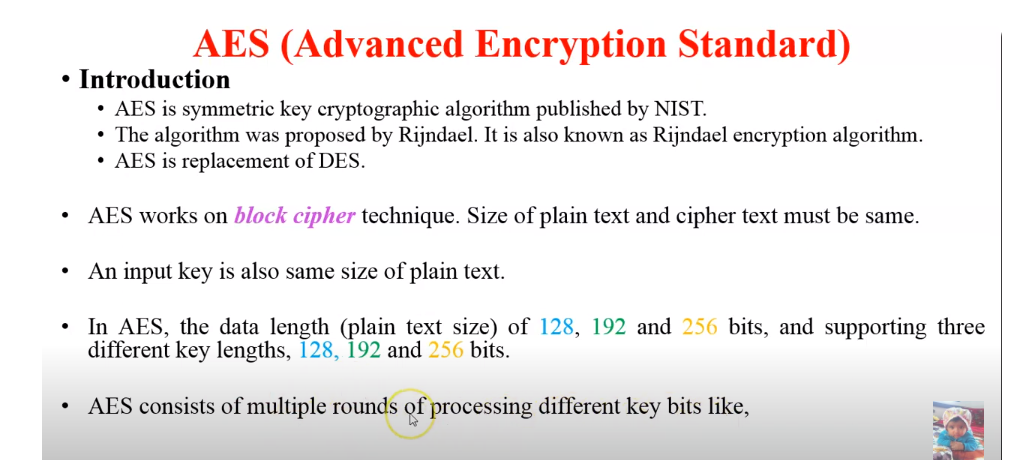
ciphertext in “blocks.” Its origins trace back to the Data Encryption Standard (DES), which

was developed in the early 1970s. DES was one of the earliest symmetric encryption

algorithms that generated 64-bit keys. A bit is the smallest unit of data measurement on a

computer. As you might imagine, Triple DES generates keys that are 192 bits, or three times

as long. Despite the longer keys, many organizations are moving away from using Triple

p

DES due to limitations on the amount of data that can be encrypted. However, Triple DES is

likely to remain in use for backwards compatibility purposes.

** Advanced Encryption Standard (AES) is** one of the most secure symmetric algorithms today.

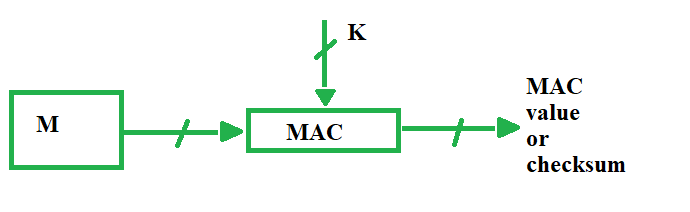
AES generates keys that are 128, 192, or 256 bits. Cryptographic keys of this size are

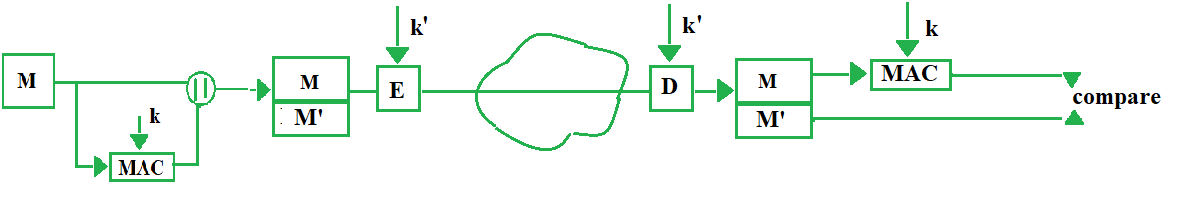
considered to be safe from brute force attacks. It’s estimated that brute forcing an AES 128-

bit key could take a modern computer billions of years!

MAC in cryptography

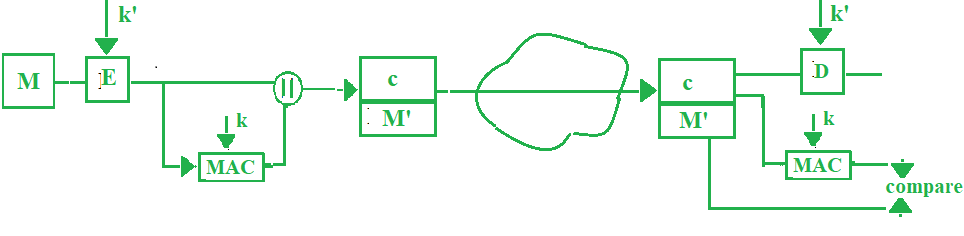
Apart from intruders, the transfer of message between two people also faces other external problems like noise, which may alter the original message constructed by the sender. To ensure that the message is not altered there’s this cool method



1. 
2. **External Error Code –** For cases when there is an alteration in message, we decrypt it for waste, to overcome that problem, we opt for external error code. Here we first apply MAC on the encrypted message ‘c’ and compare it with received MAC value on the receiver’s side and then decrypt ‘c’ if they both are same, else we simply discard the content received. Thus it saves time.

c = E(M, k')

M' = MAC(c, k)

1. 

**Problems in MAC –** If we do reverse engineering we can reach plain text or even the key. Here we have mapped input to output, to overcome this we move on to hash functions which are “One way”. **Note –** symbol “E” denotes symmetric key encryption