

31)

Compliance

This term covers the practices, guidelines and procedures required to fit security regulation, security standards of the industry, laws and guidelines to protect sensitive data.

Its essential for organisations because the lack of its implementation can lead to punitive actions as result of non accomplishment of legal obligation, loss of reputation, as result of loss of trust in the organisation and also implies the implementation of good practices regarding risk management.

32) Cryptography:

The cryptography in data security covers the practices that allow the encryption and decryption of sensitive data in storage or communication. It implements the use of private and public keys to apply the encryption and decryption processes either in synchronous or asynchronous approach.

It allows the feasibility, integrity, and security in communication as well as authentication and non-repudiation, which allows to attach a piece of data to a particular origin or source.