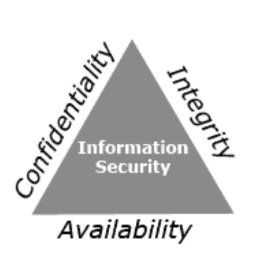
ISO/IEC 27001:2013 Information security management systems
- Information security concept-

Information security - the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information (Wikipedia)



Confidentiality
Information is not made available or disclosed to unauthorized individuals, entities, or processes.

Integrity
To maintain and assure the accuracy and completeness of data over its entire life-cycle. Data cannot be modified in an unauthorized or undetected manner.

Availability
Information is available when needed.
For information to be available it means that the computing systems that process the information and the communication channels through which information is being sent are working correctly.

ISO/IEC 27001:2013 Information security management systems
- Information security concept-

Risk - the likelihood of something happening

Risk management - the process of identifying information security risks, evaluating them and dealing with risks

Threat – anything that can harm an information asset (it can be man-made or a natural event)

Vulnerability - a weakness that can be used to harm an information asset.

Information asset – content of valuable information and the hardware or software where it is contained