INFOSEC

**Information Assurance** - the **practice of assuring** information and managing risks.

* Information assurance includes protection of the integrity, availability, authenticity, non-repudiation and confidentiality of user data.

**Why Information security is needed?**

* **IA** **( Information Assurance )** increases the utility of information to authorized users and reduces the utility of information to those unauthorized.
* **DFCSC ( Digital Forensic and Cyber Security Center )** stated that “IA practitioners must consider corporate governance issues such as privacy, regulatory and standards compliance, auditing, business continuity, and disaster recovery as they relate to information systems.

**Information Assurance process**

1. Enumeration and classification of the information assets to be protected.
2. Next, the IA practitioner will perform a risk assessment for those assets.
3. Vulnerabilities in the information assets are determined in order to enumerate the threats capable of exploiting the assets.
4. Consider the probability of a threat exploiting vulnerability in an asset.
5. Impact of a threat exploiting vulnerability in an asset, with impact usually measured in terms of cost to the asset's stakeholders.
6. The sum of the products of the threats' impact and the probability of their occurring is the total risk to the information asset.

**5 Information Assurance Pillars**

* **Availability** - means ensuring timely and reliable access to and use of information.
* **Integrity -** means protecting against improper information modification or damage.
  + assurance that the information is trustworthy and accurate.
  + involves maintaining the **consistency, accuracy, and trustworthiness** of data over its entire life cycle.
* **Authentication -** is the process of determining whether someone (or something) is, in fact, who (or what) it is declared to be.
* **Confidentiality -** means preserving authorized restrictions on access and disclosure.
  + is a set of rules that limits access to information.
* **Non-repudiation** - is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data.

**Information Security ( InfoSec** ) -, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

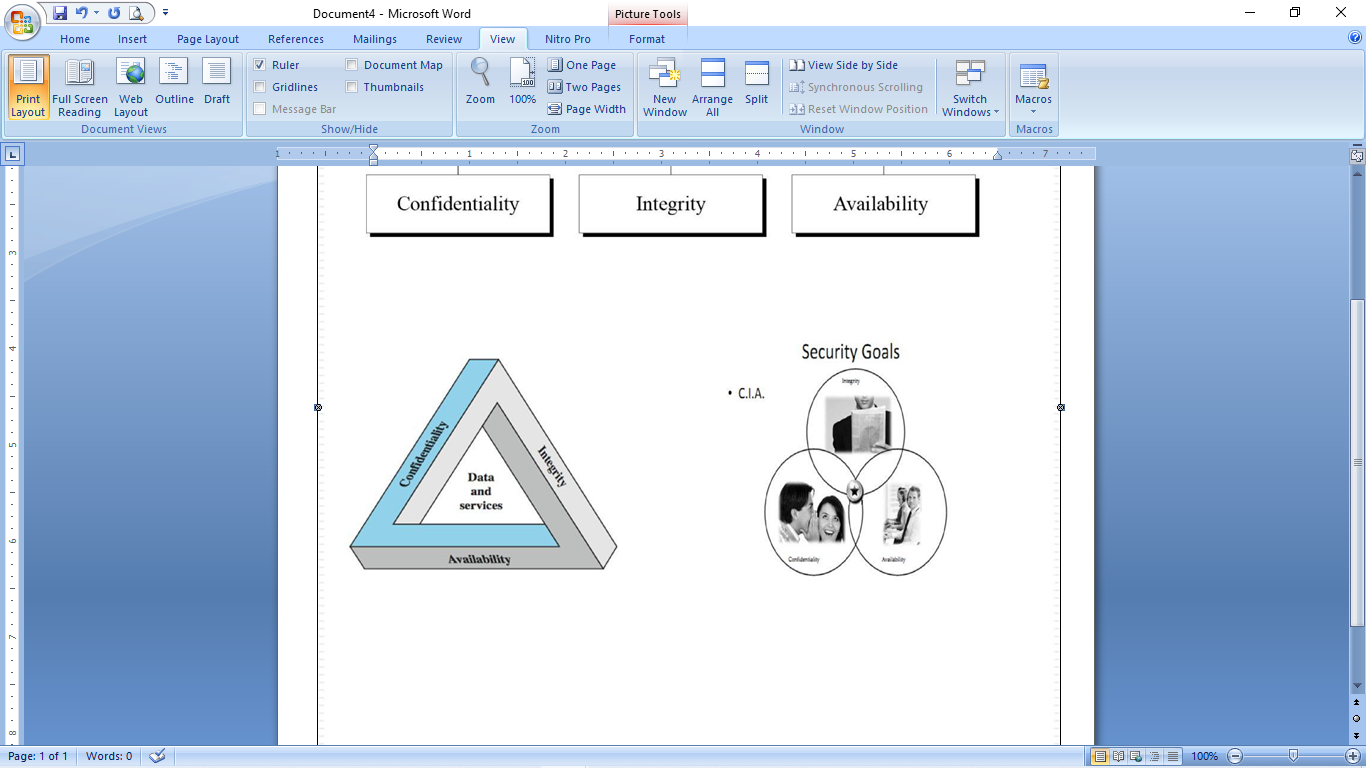
**Two major aspects of InfoSec:**

**IT Security** - Sometimes referred to as computer security, Information Technology Security is information security applied to technology.

**Information Assurance -** act of ensuring that data is not lost when critical issues arise.

**Principles of security**

These three concepts form what is often referred to as the CIA triad.



* protection of personal data **(privacy)**
* protection of data belonging to an organization **(secrecy).**

**Cyber defense -** is a computer network defense mechanism which includes response to actions and critical infrastructure protection and information assurance for organizations, government entities and other possible networks.