What is Information Assurance (IA)?

Information assurance can be called a practice of assuring and managing the risks related to confidential information, throughout the process of transmission, processing, and storing data. Information assurance is mostly focused on the protection of the integrity, availability, authenticity, non-repudiation, and confidentiality of data in the system. It does not only encompass the digital data protection but also included physical techniques.

Process of identifying and managing information-related risks as well as the procedures required to secure information systems like computers and networks.

Refers to the practice of ensuring the confidentiality, integrity, availability, and non-repudiation of essential information and associated information systems. It is a strategic process that focuses on policy deployment rather than infrastructure development.

UNDERSTANDING THE C.I.A.

CONFIDENTIALITY - Ensures that information is only accessible to those authorized to access it.
INTEGRITY - Ensures that accuracy and trustworthiness of the data
AVAILABILITY - Ensures that information and resources are accessible and usable when needed.

ASPECT OF INFORMATION THAT NEEDS PROTECTION

Integrity – refers to the confidence that all information systems are safe and secure. IA strives to ensure integrity by installing anti-virus software on all computer systems and ensuring that all employees with access understand how to use their systems properly to prevent malware and viruses from accessing information systems.

Availability – The term 'availability' refers to the capacity of individuals who require information to obtain it. Only individuals who are aware of the hazards connected with information systems should have access to it.

3. Authentication – Authentication entails verifying that persons with access to data are who they claim to be. Two-factor authentication, strong passwords, biometrics, and other devices are examples of ways to improve authentication. Not only may authentication be used to identify individuals, but it can also be used to identify other devices.

Confidentiality – Information security is concerned with information secrecy, which means that only those with permission may read sensitive data.

Non-repudiation – The last pillar states that anybody with access to your organization's information system cannot deny doing a task within it since there should be procedures in place to confirm that they did so.

What is Information Security (IS)?

Information security is a practice of protecting information by mitigating information risks. Typically, it involves reducing the probability of unauthorized access to data, or illegal use of it. Also, as the disruption,detection, modification, inspection, or recording of confidential information. It includes taking actions to prevent such incidents. The main focus of information security is providing balanced protection against cyber-attacks and hacking while maintaining confidentiality, integrity, and availability of data.

The network security includes:

1. Protection − The user needs to be capable of configuring their devices and networks accurately.

2. Detection − The user should detect whether the configuration has been modified or get a notification if there are some issues in the network traffic.

3. Reaction − After detecting the issues, the user should acknowledge them and should return to a protected position as rapidly as available.

DIFFERENCE BETWEEN IA AND IS

Information security and information assurance have slightly different objectives. In essence, the extent of what they are attempting to safeguard differs between the two.

The prevention and defense against assaults and illegal use of computer systems including networks, programs,and data, is known as Information Security. The Safeguarding of digital and non-digital information assets is known as Information Assurance.

Physical security refers to the protection of personnel,hardware, software, networks, and data from physical threats and events that could cause significant loss or harm to an enterprise, agency, or organization.

Logical security refers to the process of using software-based techniques to authenticate a user's privileges on a specific computer network or system.

Password authentication is the most common and well-known type of logical security. Anyone who has ever used an online banking site or a social networking system will be well-known with this concept.

Classification of Information in IS

Information classification is a process in information security that categorizes data based on its sensitivity and importance. The goal of classification is to protect sensitive information by applying appropriate security measures based on the level of risk associated with the data.

Public – Information that is not sensitive and can be
shared freely with anyone.

Internal – Information that is sensitive but not criticaland should only be shared within the organization.

Confidential - Information that is sensitive and requires protection, and should only be shared with authorized individuals or groups.

Secret - Information that is extremely sensitive and requires the highest level of protection, and should only be shared with a select group of authorized individuals.

Top Secret - Information that if disclosed would cause exceptionally grave damage to the national security and access to this information is restricted to a very small number of authorized individuals with a need-to-know.

Levels in Government Organization for Information Classification:

Unclassified – Information that is neither sensitive nor classified. The public release of this information does not violate confidentiality.

Sensitive but Unclassified – Information that has been designed as a major secret but may not create serious damage if disclosed.

Confidential – The unauthorized disclosure of confidential information could cause some damage to the country's national security.

Secret – Information that is extremely sensitive and requires the highest level of protection, and should only be shared with a select group of authorized individuals.

Top Secret – this is the highest level of information classification. Any unauthorized disclosure of top-secret information will cause grave damage to the country's national security.

Levels in Private Organizations for Information Classification:

Public – information that is similar to unclassified information. However, if it is disclosed, it is not expected to seriously impact the company.

Sensitive – information that required a higher level of classification than normal data. This information is protected from a loss of confidentiality as well as from loss of integrity owing to an unauthorized alteration.

Private – considered of a personal nature and is intended for company use only, its disclosure could adversely affect the company or its employee salary levels and medical information could be considered as examples of“private information”.

Criteria for Information Classification:

Value – It is the most commonly used criteria for classifying data in the private sector. If the information is valuable to an organization it needs to be classified.

Age – The classification of the information may be lowered if the information value decreases over time.

Useful Life – Information will be more useful if it will be available to make the changes as per requirements than, it will be more useful.

Personal Association – If the information is personally associated with a specific individual or is addressed by a privacy law then it may need to be classified.