kashif.nth@aup.edu.pk

CIA TRIAD

LECTURE 02

- Kashif Ali
- BSCS 5th FGHI

- Subject: Information Security

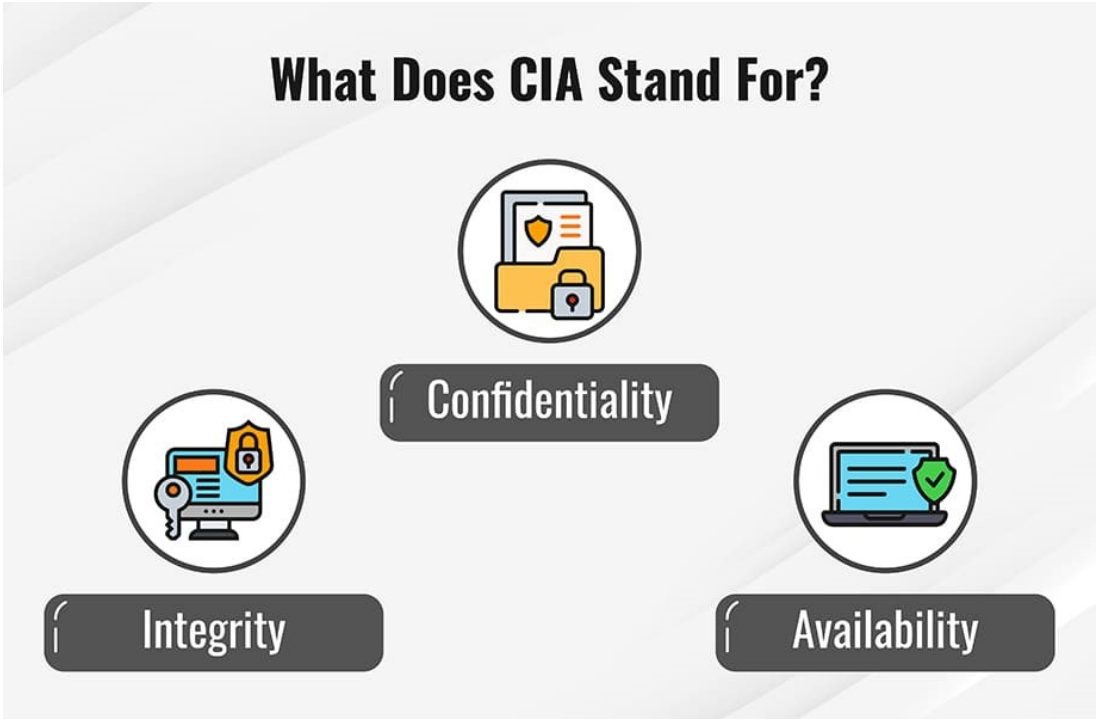
kashif.nth@aup.edu.pk

What is the CIA Triad?

- The three letters in "CIA triad" stand for Confidentiality, Integrity, and Availability. The CIA triad is a common model that forms the basis for the development of security systems. They are used for finding vulnerabilities and methods for creating solutions.

- The confidentiality, integrity, and availability of information is crucial to the operation of a business, and the CIA triad segments these three ideas into separate focal points. This differentiation is helpful because it helps guide security teams as they pinpoint the different ways in which they can address each concern.

- Ideally, when all three standards have been met, the security profile of the organization is stronger and better equipped to handle threat incidents.



Confidentiality

- Confidentiality involves the efforts of an organization to make sure data is kept secret or private. To accomplish this, access to information must be controlled to prevent the unauthorized sharing of data—whether intentional or accidental.
- A key component of maintaining confidentiality is making sure that people without proper authorization are prevented from accessing assets important to your business. Conversely, an effective system also ensures that those who need to have access have the necessary privileges.

Confidentiality (continued)

- To fight against confidentiality breaches, you can classify and label restricted data, enable access control policies, encrypt data, and use multi-factor authentication (MFA) systems.
- It is also advisable to ensure that all in the organization have the training and knowledge they need to recognize the dangers and avoid them.

Integrity

- Integrity (or data integrity) is the accuracy and consistency of data as well as the completeness and reliability of systems.
- It means that data is complete and accurate from its original form.
- Integrity involves making sure your data is trustworthy and free from tampering.
- The integrity of your data is maintained only if the data is authentic, accurate, and reliable.

Integrity (continued)

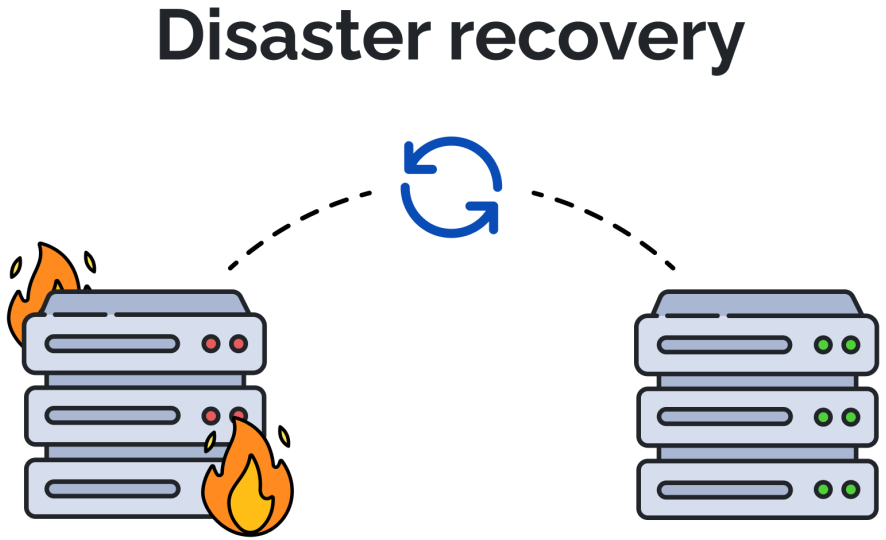
- To protect the integrity of your data, you can use hashing, encryption, digital certificates, or digital signatures.
- For websites, you can employ trustworthy certificate authorities (CAs) that verify the authenticity of your website so visitors know they are getting the site they intended to visit.

Availability

- Availability refers to maintaining the ability to access your resources when needed, even under duress (like a natural disaster) or after suffering intentional cyberattacks.
- Availability means guaranteeing reliable access to information by authorised personnel.
- Even if data is kept confidential and its integrity maintained, it is often useless unless it is available to those in the organization and the customers they serve.
- This means that systems, networks, and applications must be functioning as they should and when they should.

Availability (continued)

- To ensure availability, organizations can use redundant networks, servers, and applications.
- These can be programmed to become available when the primary system has been disrupted or broken.
- You can also enhance availability by staying on top of upgrades to software packages and security systems.
- Backups and full disaster recovery plans also help a company regain availability soon after a negative event.



https://www.fortinet.com/resources/cyberglossary/cia-triad#:~:text=The%20three%20letters%20in%20%22CIA,and%20methods%20for%20creating%20solutions.


Any Questions