

CIA Triad Summary

The CIA Triad is a model for information security within organizations. It provides guidelines to ensure that data is safe, protected, and available. There are 3 main concepts, Confidentiality, Integrity, and Availability.

> Confidentiality

> What it is:

Confidentiality ensures that data is only accessible by those with the correct permissions.

> What it does:

It prevents unauthorized sources from accessing the information. Think of it like a password to a safe. It is needed to access the contents.

> What it doesn't:

Confidentiality doesn't protect the data from any tampering. If you are allowed to access it, you have full control. It also isn't guaranteed to be available at all times.

> Integrity

> What it is:

Integrity ensures the data remains as it was, and cannot be altered.

> What it does:

It prevents unauthorized tampering of data, such as a rogue employee or a piece of bad software.

> What it doesn't:

Integrity doesn't guard against unauthorized access, just illegal tampering. It also doesn't ensure the data is available.

> Availability

> What it is:

Availability ensures the data is consistently accessible and available.

> What it does:

It provides the guarantee that the data will be available when needed, such as providing multiple servers with the same copy of data so that, if one goes down, the data is still accessible.

> What it doesn't:

Availability doesn't guard against unauthorized access or modification.

Each CIA triad concept is just one pillar that, when combined with the others, provides a safe and reliable data storage method. Confidentiality and Availability can't guard against tampering, but Integrity can. Integrity and Availability can't guard against unauthorized access, but Confidentiality can. Availability and Confidentiality can't ensure the data is unmodifiable, but Integrity can. Together, they help keep data safe globally.

Source:

["What is the CIA Triad? Definition, Explanation, Examples" - Wesley Chai](#)