

Write up on the Cia Triad
By Vincent Saunders
CYSE 200T

Three important concepts known as the "CIA Triad," which is a core premise in information security, should ensure the confidentiality, integrity, and availability of an organization's data and information systems.

The idea of secrecy ensures that only authorized persons or systems have access to information. It comprises preventing unauthorized access or disclosure of sensitive data. Confidentiality measures are intended to prevent data breaches and illegal information releases. Integrity ensures the accuracy and dependability of data and information systems. It comprises safeguarding data from unauthorized changes, whether purposeful or inadvertent. It is ensured that the data is reliable and unaffected by protecting data integrity. Availability ensures that data and systems are accessible and functional when needed. It comprises preventing delays or downtime that can have an impact on an organization's ability to carry out its operations. Availability metrics strive to ensure the dependability and consistency of systems and data.

In order to access any specific asset or system, an individual or entity's identification needs to be verified through the process known as authentication. The intention is to prove that the network or person looking to gain access is exactly what they say they are. The most popular ways of authenticating used today are usernames and passwords, biometrics like fingerprint and face inspection, smart cards, and two-factor authentication. A user attempting to access the financial database would serve as an example of authentication. There is a username and password provided. The system checks these credentials to authenticate the user's identity. If the credentials match, authentication is successful and the user's identity is known to the system.

A person or system is permitted to access certain resources or execute specific tasks after authentication. It creates rights and benefits based on recognized identification. Authorization ensures that users have the appropriate access privileges and can only perform or access resources for which they have been granted authorization. Following authentication, the system determines what the user is capable of doing in the financial database. For example, the user may be able to see financial reports but not to edit the data. Another user in a different role may be granted authority to change financial data. These access permissions are determined by authorization based on the user's position and responsibilities inside the organization.

Reference page

"Authentication" - NIST Special Publication 800-63B: "Digital Identity Guidelines."

"Authorization" - NIST Special Publication 800-53: "Security and Privacy Controls for Federal Information Systems and Organizations."