A Description of the CIA Triad

Kevin A. Loarca

Old Dominion University

CYSE 200T: Cybersecurity, Technology & Society

Professor Christopher Bowman

June 07, 2026

A Description of the CIA Triad

The CIA Triad stands for confidentiality, integrity, and availability. This is a model that is designed as guidance for organizations to create policies for information security ("What is the CIA Triad? Definition, Explanation, Examples," n.d.). It is used for finding vulnerabilities and methods for creating solutions ("CIA triad," n.d.). These methods guide security teams as they pinpoint different ways to address each concern ("CIA triad," n.d.). The first concept, confidentiality, is designed to prevent sensitive information from unauthorized access attempts ("What is the CIA Triad? Definition, Explanation, Examples," n.d.). The second concept, integrity, involves maintaining a consistent, accurate, and trustworthy of data over its entire lifecycle ("What is the CIA Triad? Definition, Explanation, Examples," n.d.). The data during transit must not be changed, and security implementations must be done to ensure it is not altered by an unauthorized person. The third concept, availability, is defined as information being consistent and ready for access to authorized individuals. This is done by maintaining hardware and technical infrastructure and systems that hold and display information ("What is the CIA Triad? Definition, Explanation, Examples," n.d.).

Differences between Authentication and Authorization

Between these two concepts, they have differences, which improve security. The purpose of authentication revolves around verifying who you are, while the other determines what the user is allowed to do ("Authentication vs authorization," 2026). The verification, in authentication, is done to identify a user before granting them access to the system. An example of this could be the requirement of credentials, such as a password or biometrics ("Authentication vs authorization," 2026). Once the user is verified, they are then set to the next step of authorization. In this step, the user is given resources that they are allowed to access and

actions that they are allowed to perform ("Authentication vs authorization," 2026). To give an example, a system administrator only allows authorized users from the financial department to access their given resources and not the HR department's computers.

Conclusion

The CIA triad guides security experts to pinpoint concerns in security that will address issues differently. Confidentiality only allows authorized users to view sensitive information. Integrity involves keeping data, while in transmission, the same and preventing any tampering from unauthorized users. Lastly, availability is defined as data being readily available for authorized users to access. This guide then highlights two additional concepts that can be seen. There is authentication, which verifies who the user is by requiring them to use credentials to access systems. Once allowed in, authorization gives users limited access to what they can view and perform on selected systems. In the end, these security measures and additional steps are needed to perform the right amount of security to protect systems.

References

Authentication vs authorization. (2026, March 31). GeeksforGeeks. https://www.geeksforgeeks.org/computer-networks/difference-between-authentication-and-authorization/

CIA triad. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/cia-triad

What is the CIA Triad_ definition, explanation, examples - TechTarget.pdf. (n.d.). Google Docs. https://drive.google.com/file/d/1898r4pGpKHN6bmKcwlxPdVZpCC6Moy8l/view