

**The CIA Triad**

Arielle C. Chapman

School of Cybersecurity, Old Dominion University

CYSE200T

Mr. Charles E. Kirkpatrick

September 17, 2023

*The CIA Triad is an integral framework for the security of data which breaks down the hefty task of cybersecurity into three components. Along with the CIA Triad, authentication and authorization preserve the efforts of the CIA Triad. Together, they are a quintet of upspoken cyber law that is efficient and proven best to protect data.*

## **What is the CIA Triad**

The CIA Triad stands for confidentiality, integrity and availability. This is a crucial trio, especially in the information security field, because “[e]very cyber-attack attempts to violate at least one of the CIA triad attributes,” (Election Security Spotlight). Broken down, the foremost value of the triad is confidentiality, which is parallel to privacy. It ensures that personal data can only be read by authorized personnel. An example of a confidentiality measure is the implementation of two-factor identity, or 2FA. Integrity is the maintenance of information during its life cycle. This means that data traveling through the system is not intercepted, changed in transit, or altered in any way. Establishing integrity, for example, can look like a company using backup and recovery software to protect every byte of data that goes through their systems. Availability describes the access to up-to-date resources necessary for cyber protection, and the accessibility of data in an authorized request. This component can be seen as ensuring systems, hardware, and applications stay updated. With the CIA triad, security experts can better understand, protect against, identify, and investigate network risks. It standardizes the cybersecurity conversation in organizations as to prioritize the demands of each component.

## **Authentication vs Authorization**

When used in tandem with the CIA Triad, both authentication and authorization can reinforce access control. However, it’s important to realize and understand that they are not the same thing. Authentication is the assurance that someone is who they say they are. As an example, if you present your state-issued ID and passport at an airport, you are being authenticated. You should be the only one with an authentic copy of those two items. Alternatively, authorization is the process by which previously authenticated users access data based on their permissions. For example, someone who is confirmed to be an accountant should have financial databases available to them, but not access to customer information.

## **Conclusion**

The CIA Triad lays a crucial foundation for the security of multiple, if not all, fields and industry in the modern world. In collaboration with both authentication and authorization techniques, these concepts arrange and upgrade the state of cybersecurity in an organization.

## References

Auth0. (n.d.). Authentication vs. Authorization. Auth0 Docs. <https://auth0.com/docs/get-started/identity-fundamentals/authentication-and-authorization>

Election Security Spotlight – CIA Triad. (n.d.). CIS. <https://www.cisecurity.org/insights/spotlight/ei-isac-cybersecurity-spotlight-cia-triad>

What is the CIA Triad? Definition, Explanation, Examples - TechTarget. (n.d.). WhatIs.com. <https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA?jr=on>