

Write Up: The CIA Triad

Jacob M. Shaylor

Old Dominion University

CYSE200T Cybersecurity, Technology, Society

Prof. Bowman

June 7th, 2026

The CIA Triad

The CIA Triad is known as the foundational guide to information security practices. According to Chai, it consists of three major principles: Confidentiality, Integrity, and Availability. These components each help organizations prevent sensitive data from falling into the wrong hands, also known as unauthorized users. It does so by maintaining consistency of the data and ensuring that the data is readily accessible to those who are authorized to view it. It is also important to understand the difference between authentication and authorization. Let's start with breaking down the CIA Triad.

Confidentiality

The first leg of the CIA Triad, confidentiality, ensures that sensitive data is only attainable by authorized personnel. This can be achieved by methods such as encryption, password protected files or information systems, and authentication factors. This prevents unauthorized users from accessing important, sensitive data and allows for verification procedures to be met to ensure that the right people are accessing the data. An example of this could be a school employee who has to use county issued credentials to log in and access student records. This will protect students from having their information viewed by someone who is not authorized to do so by the school system.

Integrity

The integrity piece of the CIA Triad works to maintain accurate, consistent data. Files can include checksums, or a string of numbers and letters used to identify the originality of the file. This acts as a digital fingerprint, any alterations to the checksum will indicate that the file has been changed or modified. Digital signatures are also very important. This records authorized users when they make a change. This helps maintain the integrity of the data that is

being protected and accessed by authorized users. An example of this would be a patient's health chart. When a doctor prescribes medication, there usually is a digital signature indicating who made the change.

Availability

The final portion of the CIA Triad is availability. Availability relates to being able to access systems and softwares when needed. The way this can be achieved is by ensuring that hardware is up to date and any needed repairs are noted and completed. To keep availability functioning at its highest, software updates need to be kept up with. This piece is all about the systems you are using and making sure that the physical equipment and software are operating as they should be. An example of this would be an e-commerce business keeping their website operational so that users can view products and make purchases.

Authentication vs Authorization

While these topics do play hand in hand with each other, there is a big difference. Put simply, authentication verifies a user's identity. Whether it be by password requirements, biometrics, or collection of other personal data such as a social security number, one must meet requirements to verify their identity. An example of this is having to input a username and password combination to access your company's laptop. The username and password verifies the user who is then allowed to log into the laptop. Authorization on the other hand allows a user to access certain pieces of information. For example, once you log into your company's laptop, you are only authorized to see data pertinent to your job. As a school employee, because of my role as a security officer, I have access to all student files, demographics, emergency contacts, and address information enrolled in our school as well as county wide. Whereas a teacher in my school only has access to the students in his or her class.

References

Chai, W. (2023, December 21). What is the CIA Triad (confidentiality, integrity and availability)

TechTarget.

<https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-C>

IA

IBM. (2025). Authentication vs. authorization: What's the difference? IBM.

<https://www.ibm.com/think/topics/authentication-vs-authorization>