Ava Love Dimaiwat

9/14/2025

CYSE-200

# The CIA Triad

## What is the CIA Triad?

The CIA (or AIC) Triad is a foundational model in information security and it stands for Confidentiality, Integrity, and Availability. This model is very important because it helps to guide organizations to build strategies and policies that protect data by focusing on these components of the Triad.

## Confidentiality

Confidentiality is important to make sure that information and data is accessible to only those who are authorized. According to SentinelOne in "*What is the CIA Triad?"* it protects any sensitive data such as medical records, passwords, and financial information from being stolen or seen by the wrong people. This is similar to going to the bank and having different security methods to make sure your personal information and data is only accessible to you (and the bank). This can be done with techniques like encryption, strong passwords, and access controls (Chai, 2022).

## Integrity

Integrity ensures that the data remains accurate and unaltered. This can be checked with things like digital signatures, checksums, and version control to verify that information hasn't been modified (Chai, 2022). In healthcare, integrity safeguards are to prevent unauthorized changes in medical records.

## Availability

Availability makes sure that information systems are accessible to authorized users when needed. This can be best ensured by keeping check of hardware and doing hardware repairs when needed for a fully functional operating system (OS).This is done through redundancy, disaster recovery planes, and defenses against denial-of-service (DoS) attacks (Chair, 2022). For example, cloud storage providers use multiple servers to make sure there's availability even in case of an outage.

## Authentication vs. Authorization

These two terms are usually used together but have different uses in cybersecurity. In *Authentication vs. Authorization: Key Roles in Access Control*, Phillip Shoemaker states, "Authentication is used to verify a user's identity, while authorization determines what resources that verified user can access."

### Authentication

This is the process of verifying a user's identity through credentials like passwords, tokens, or biometrics. If these credentials match stored records, access is granted. This is important to prevent unauthorized access, fraud, and data breaches. This also helps organizations protect sensitive data and IT systems (Shoemaker, 2025).

The most common authentication is password authentication, it requires a username and password. Students use this to log into their computers and accounts like google, canvas, and microsoft. Another type of authentication used is Two-Factor Authentication (2FA), this requires additional verification like one-time passwords, sending a code to your phone number, or authentication apps. An authentication app that ODU students use all the time is Duo-Push, this is usually used when logging in to a device that you don't own, and is done so other users on the device can't access your accounts.

**Authorization**

Authorization defines what actions an authenticated user can do by controlling access levels and permissions, typically through role or policy-based rules. It helps protect sensitive data by preventing unauthorized activities and reducing insider threats (Shoemaker, 2025).

Organizations employ different authorization models to manage their user permissions. This includes Role-Based Access Control (RBAC), Discretionary Access Control (DAC), Attribute-Based Access Control (ABAC), and Mandatory Access Control (MAC).

## Conclusion

The CIA Triad, authentication, and authorization makes the foundation of cybersecurity. Confidentiality, integrity, and availability ensures that data is protected, accurate, and accessible. Authentication and authorization work together to control who can access systems and what they are allowed to do. Together, these principles provide organizations with the tools to safeguard sensitive information and maintain secure operations in an increasingly digital world.