

Lydia Robb  
CYSE 200T  
Sept 14, 2025  
Professor Duvall

## **CIA Triad and Authentication vs. Authorization**

### **BLUF:**

The CIA Triad is the foundation of information security. It guides organizations in safeguarding data against unauthorized access, tampering, and disruption. In parallel, understanding the difference between authentication (verifying identity) and authorization (defining permissions) is critical for implementing effective access control. Together, these principles ensure data remains secure, reliable, and usable.

### **The CIA Triad**

The CIA Triad is essentially a framework to maintain security, especially in the cyber realm. CIA stands for confidentiality, integrity, and availability. These are listed in order of defense but are also intertwined in the overall functionality of security. I will go on to list each aspect of the triad and its function in some detail.

### **Confidentiality**

Confidentiality focuses on protecting information from unauthorized access and disclosure. It ensures that sensitive data is only available to individuals or systems with the proper permissions. Methods like encryption, access controls, authentication, and secure passwords are commonly used to maintain confidentiality. By safeguarding information from leaks or breaches, organizations can preserve privacy, maintain trust, and reduce the risk of cyberattacks or data misuse (Chai, 2022).

### **Integrity**

Integrity ensures that information remains accurate, reliable, and unaltered except by authorized individuals or processes. It focuses on protecting data from unauthorized modifications, whether accidental or malicious, so that users can trust the information they are working with. Techniques such as checksums, hashing, digital signatures, and version control help maintain integrity by detecting and preventing unauthorized changes. By safeguarding integrity, organizations ensure that decisions and operations are based on correct and trustworthy information (Chai, 2022).

## Availability

Availability ensures that information and systems are accessible to authorized users whenever needed. It focuses on keeping data, networks, and resources reliable and functional, even during unexpected disruptions like hardware failures, cyberattacks, or natural disasters. Measures such as redundancy, regular backups, disaster recovery plans, and robust security protections help maintain availability. By ensuring consistent access, organizations can support business operations, prevent downtime, and provide users with the resources they depend on (Chai, 2022).

## Authentication vs. Authorization

While the CIA Triad outlines the goals of information security, authentication and authorization explain how access is controlled in practice. Authentication verifies identity, for example, entering a username and password or using biometrics to log in confirms that a person is who they claim to be (IBM, 2023). Authorization then determines what that authenticated user is allowed to do, enforcing the principle of least privilege so users only access resources appropriate to their role (Microsoft, 2024). A hospital system provides a clear example. For instance, both a doctor and a receptionist authenticate by logging in with their credentials, but authorization grants the doctor access to patient medical records while restricting the receptionist to appointment schedules. This combination ensures sensitive information is protected while still supporting operational needs.

## Conclusion

In conclusion, the CIA Triad serves as a fundamental framework for understanding and practicing cybersecurity. Each component plays a critical role, as confidentiality protects privacy, integrity ensures data remains accurate and trustworthy, and availability keeps systems and information accessible to authorized users. Together with authentication and authorization, the triad provides the foundation for secure systems and safe digital practices. It is essential knowledge for anyone entering the field of IT or cybersecurity.

## References

Chai, W. (2022, June 28). *What is the CIA triad? Definition, explanation, examples*. TechTarget. <https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA>

IBM. (2023, March 15). *Authentication vs. authorization: What's the difference?* IBM Security. <https://www.ibm.com/topics/authentication-vs-authorization>

Microsoft. (2024). *Authorization basics*. Microsoft Learn. <https://learn.microsoft.com/en-us/azure/active-directory/develop/authorization-basics>

