Honesty Alexander

6/7/2026

The CIA Triad

What is the CIA Triad?

The CIA Triad stands for Confidentiality, Integrity, and Availability, which are considered the three foundational principles of cybersecurity and information security (Aldabagh, 2025). The concept of the CIA Triad developed over time and does not have a single creator. The idea of confidentiality may have first appeared in a 1976 U.S. Air Force study, while the concept of integrity was discussed in a 1987 paper by David Clark and David Wilson that emphasized the importance of accurate and trustworthy data in commercial computing (Chai, 2022). The concept of availability became more widely recognized in 1988, and by 1998 these three principles were commonly grouped together as the CIA Triad. Today, organizations use this model to guide security policies and protect sensitive information from threats, unauthorized access, and data loss.

Confidentiality refers to keeping information private and ensuring that only authorized individuals can access it. Examples of confidentiality include strong passwords, encryption, biometric verification, account numbers, and two-factor authentication (Chai, 2022). These security measures help prevent sensitive information from falling into the wrong hands and protect users from threats such as identity theft and unauthorized account access. Integrity focuses on maintaining the accuracy, consistency, and trustworthiness of information throughout its entire lifecycle. Organizations use file permissions, access controls, version control systems, digital signatures, checksums, and backups to ensure that data is not altered, deleted, or corrupted by unauthorized users. Availability ensures that information and systems are accessible to

authorized users whenever they are needed. This principle is supported through regular hardware maintenance, software updates, backups, disaster recovery plans, redundancy systems, and protection against cyberattacks that could cause downtime (Aldabagh, 2025).

The three components of the CIA Triad work together to create a strong security framework. For example, an online banking system protects customer information through confidentiality measures such as passwords and encryption, maintains integrity by ensuring account balances and transaction records remain accurate, and provides availability by allowing customers to access their accounts whenever needed through reliable systems. One major advantage of the CIA Triad is that it provides organizations with a simple and effective framework for evaluating and improving cybersecurity practices (Aldabagh, 2025). It helps businesses identify security weaknesses while ensuring that information remains protected, accurate, and available. Another advantage is that it encourages organizations to consider security as a complete system rather than focusing on only one area. However, implementing all three principles can be expensive, time-consuming, and technically challenging. In addition, cybersecurity threats continue to evolve, leading some experts to believe that the model may need updates to address modern security concerns (Chai, 2022). Despite these challenges, the CIA Triad remains extremely important because it serves as the foundation of information security, helps organizations reduce risks, protects sensitive data, and maintains trust between businesses and their customers.

Differences between Authentication and Authorization

Authentication and authorization are both important parts of information security, but they serve different purposes. Authentication is the process of verifying a user's identity, usually

through methods like usernames and passwords. It can also include stronger methods like two-factor authentication, biometric verification, and security tokens such as key fobs or soft tokens(Chai, 2022). These methods help ensure that the person trying to access a system is actually who they claim to be. Overall, authentication is focused on protecting systems by confirming identity before access is granted.

Authorization, on the other hand, determines what an authenticated user is allowed to do once they are inside a system (Chai, 2022). It uses tools like file permissions, user access controls, and version control to limit what information someone can view or change. This helps ensure that even authorized users only access the data they are permitted to use. Authorization is important for maintaining confidentiality, integrity, and proper data handling within an organization. Overall, it controls access levels after a user's identity has already been verified. (Aldabagh, 2025).

References

Aldabagh, H., Bowman, C., Kirkpatrick, C., Oesteraas, I., & Diwakar Yalp, V. L. (2025). *Cybersecurity, Technology, Society: A Multi-Disciplinary Look at the Field of Cybersecurity: Chapter 2* https://app.perusall.com/courses/202530_cyse200t_33004-cybersecurity-technol-society/cybersecurity-technology-and-society-first-edition-2025?filter=all

Chai, W. (2022). *What is the CIA Triad? Definition, Explanation, Examples* [Review of *What is the CIA Triad? Definition, Explanation, Examples*]. https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA?jr=on