

Sean Shreve

12FEB2026

CYSE 200T

Professor Duvall

Write-Up: The CIA Triad

BLUF: The CIA Triad consists of three main criteria: confidentiality, integrity, and availability.

These three criteria encompass an overarching model for policies and information security within a company or organization. This paper will define each element and why it is important.

The CIA Triad

The CIA Triad consists of confidentiality, integrity and availability. These core principles provide guidance to have an effective cybersecurity policy in an information systems setup. Combined, they form a framework that evaluates risk, implements security functions, and protects against unauthorized access methods (Chai, 2022).

Confidentiality

Confidentiality reaffirms sensitive information is accessible only to authorized individuals. Its focus is preventing unauthorized disclosure of data. Some examples of confidentiality include strong password requirements, encryption of data, and multi-factor authentication.

Integrity

Integrity involves maintaining the structure of the data that is being secured. Preventing unauthorized changes to the data is paramount. If integrity is at risk, data may be corrupted,

which can lead to system failures. Examples of system tools that uphold integrity include checksums and digital signature methods.

Availability

Availability's main role is ensuring that users have access to data and the systems they use in the organization or business. To maintain availability, routine maintenance of systems is essential. Updating hardware, operational software, and implementation of failsafes can help bolster availability's uptime (Chai, 2022). An example of protecting availability would be backups of the server settings of a business in case of a hack.

Differences Between Authentication & Authorization

The differences between authentication and authorization are tied to the what and the who in a security setting. Authentication is the process of verifying that the person using the system or application is who they are claiming to be. Methods include passwords, biometric scans, and smart cards.

Authorization occurs after authentication and determines what the user is allowed to access. It is typically enforced through role-based access control (RBAC), control lists, or frameworks that are policy-based (Fortinet, 2025).

Conclusion:

The CIA Triad encompasses confidentiality, integrity and availability that coalesce into a model that, when followed, can provide an excellent foundation for cybersecurity in an organization or business. Each criterion of the CIA has its own strengths and resources, and any gap in a particular aspect is covered by the other two. When specifically discussing authentication and authorization practices in the CIA framework, it's important to note that authentication must happen first to determine the user is who they claim to be. Authorization

involves what data or system the authenticated user would have access to. Utilizing all five security facets is essential for a properly secured information system to function.

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>

Fortinet. (2025). *What is the CIA Triad and why is it important?* Fortinet Cyber Glossary.

<https://www.fortinet.com/resources/cyberglossary/cia-triad>