Information Security

Domain 1 - Security & Risk Management

Topics

Information Security Concepts

Information Security Governance

Types of Attackers (Actors)

Legal and Regulatory Issues

Ethics

Access Control Defensive Categories and Types

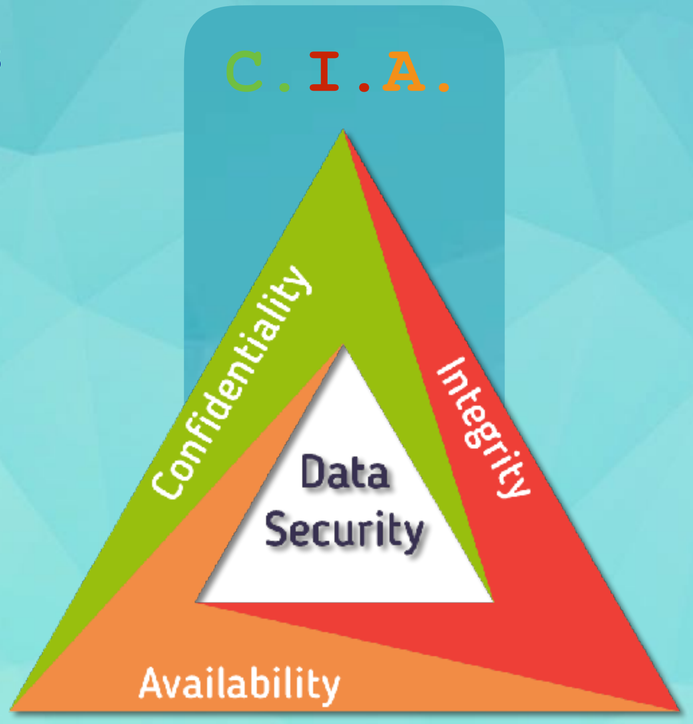
Risk Analysis

Confidentiality, Integrity, Availability

Confidentiality is the protection of information from unauthorized access

Integrity is the protection of information from unauthorized access or accidental changes

Availability is ensuring information is available and accessible to users and resources when required



Confidentiality

The most **important** aspect of information security.

Most commonly enforced through **encryption**.

Encryption should be done both for **data-in-motion (DIM)** and **data-at-rest (DAR)**.

Integrity

Ensures that only the **correct people** will be able to see privileged company information.

Enforced through a **User Access Control** system that defines permissions for who can access which data.

Extends beyond simply permissions:

- Authentication protocols
- Strong password policies
- Ensuring unused accounts (e.g., employees that have left the company) are locked or deleted

Integrity


Accuracy
Usability
Row
Count
Completeness
Consistency
Validity
Redundancy
Referential
Integrity
Domain
Integrity
Data Integrity

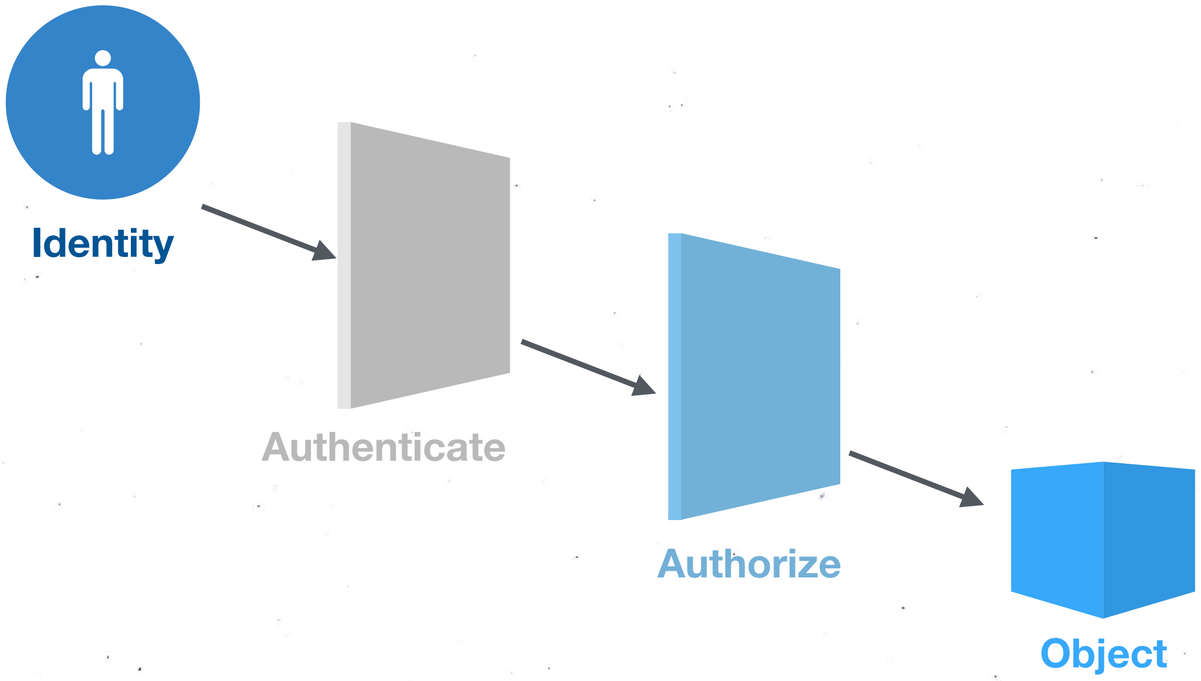
Availability

Relates to the need for databases to **be up and available** for use.

Databases need to be **dependable** in order to be functional, which requires they be up and running whenever the organization is.

This means downtimes should be **planned** on weekends and servers kept **up-to-date**.

Authentication, Authorization and Accountability (AAA)



Authentication

Relates to the need for databases to **be up and available** for use.

Databases need to be **dependable** in order to be functional, which requires they be up and running whenever the organization is.

This means downtimes should be **planned** on weekends and servers kept **up-to-date**.