### The CIA Triad: A Core Security Model

In your role as an entry-level **security analyst**, understanding and applying the **CIA triad** will be central to your responsibilities. This model helps inform how organizations manage risks while setting up systems and security policies to protect sensitive data and assets.

**What is the CIA Triad?**

The **CIA triad** stands for **Confidentiality, Integrity, and Availability**—three core principles that are critical for maintaining security.

1. **Confidentiality**
   * Ensures that only **authorized users** have access to sensitive data.
   * Sensitive data should be shared on a **"need to know" basis** to prevent unauthorized access.
   * Example: A bank must protect customers' **personal and financial information** from unauthorized access.
2. **Integrity**
   * Ensures that data is **correct, authentic**, and **reliable**.
   * Analysts must assess whether data can be trusted and verify its **authenticity**.
   * Example: If unusual behavior is detected on a bank account (like sudden changes in spending), the bank will temporarily **lock the account** to verify the **account owner’s identity**.
3. **Availability**
   * Ensures that data and systems are **accessible** to authorized users when needed.
   * Data that cannot be accessed is **useless**, and availability is essential for timely decision-making and daily operations.
   * Example: A bank invests in **robust systems** to make sure customers can access their accounts securely, at any time.

**Using the CIA Triad to Protect Your Organization**

The CIA triad plays a vital role in **defending organizations** against various **threats**, **risks**, and **vulnerabilities**. For example, when working for an organization such as a bank, each of the triad's principles is integral:

* **Confidentiality** is vital for protecting **customer privacy**.
* **Integrity** ensures data is not tampered with and is trustworthy.
* **Availability** guarantees that customers can always access their account data.

As a security analyst, constantly referring to the CIA triad will help you ensure that sensitive assets and information are protected from threats like **social engineering attacks, malware**, and **data theft**.

# Use the CIA triad to protect organizations

Previously, you were introduced to the confidentiality, integrity, and availability (CIA) triad and how it helps organizations consider and mitigate risk. In this reading, you will learn how cybersecurity analysts use the CIA triad in the workplace.

## The CIA triad for analysts

The **CIA triad** is a model that helps inform how organizations consider risk when setting up systems and security policies. It is made up of three elements that cybersecurity analysts and organizations work toward upholding: confidentiality, integrity, and availability. Maintaining an acceptable level of risk and ensuring systems and policies are designed with these elements in mind helps establish a successful **security posture**, which refers to an organization’s ability to manage its defense of critical assets and data and react to change.

### ****Confidentiality****

**Confidentiality** is the idea that only authorized users can access specific assets or data. In an organization, confidentiality can be enhanced through the implementation of design principles, such as the principle of least privilege. The principle of least privilege limits users' access to only the information they need to complete work-related tasks. Limiting access is one way of maintaining the confidentiality and security of private data.

### ****Integrity****

**Integrity** is the idea that the data is verifiably correct, authentic, and reliable. Having protocols in place to verify the authenticity of data is essential. One way to verify data integrity is through [cryptography](https://www.nist.gov/cryptography#:~:text=Cryptography%20uses%20mathematical%20techniques%20to,that%20drives%20research%20and%20innovation.)

, which is used to transform data so unauthorized parties cannot read or tamper with it (NIST, 2022). Another example of how an organization might implement integrity is by enabling encryption, which is the process of converting data from a readable format to an encoded format. Encryption can be used to prevent access and ensure data, such as messages on an organization's internal chat platform, cannot be tampered with.

### ****Availability****

**Availability** is the idea that data is accessible to those who are authorized to use it. When a system adheres to both availability and confidentiality principles, data can be used when needed. In the workplace, this could mean that the organization allows remote employees to access its internal network to perform their jobs. It’s worth noting that access to data on the internal network is still limited, depending on what type of access employees need to do their jobs. If, for example, an employee works in the organization’s accounting department, they might need access to corporate accounts but not data related to ongoing development projects.

## Key takeaways

The CIA triad is essential for establishing an organization’s security posture. Knowing what it is and how it’s applied can help you better understand how security teams work to protect organizations and the people they serve.