

confidentiality, integrity, and availability (CIA triad)



Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization. The model is also sometimes referred to as the AIC triad (availability, integrity and confidentiality) to avoid confusion with the Central Intelligence Agency. The elements of the triad are considered the [three most crucial components of security](#).

In this context, [confidentiality](#) is a set of rules that limits access to information, [integrity](#) is the assurance that the information is trustworthy and accurate, and [availability](#) is a guarantee of reliable access to the information by authorized people.

Confidentiality

Confidentiality is roughly equivalent to [privacy](#). Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people while making sure that authorized people can access it. It is common for data to be categorized according to the amount and type of damage that could be done should it fall into unintended hands. More or less stringent measures can then be implemented according to those categories.

Sometimes safeguarding data confidentiality involves special training for those privy to sensitive documents. Such training would typically include security risks that could threaten this information. Training can help familiarize authorized people with risk factors and how to guard against them. Further aspects of training may include strong passwords and password-related best practices and information about [social engineering](#) methods, to prevent users from bending data-handling rules with good intentions and potentially disastrous results.

A good example of methods used to ensure confidentiality is an account number or routing number when banking online. Data [encryption](#) is a common method of ensuring confidentiality. User IDs and [passwords](#) constitute a standard procedure; two-factor [authentication](#) is becoming the norm. Other options include [biometric verification](#) and [security tokens](#), [key fobs](#) or [soft tokens](#). In addition, users can take precautions to minimize the number of places where the information appears and the number of times it is actually transmitted to complete a required transaction. Extra measures might be taken in the case of extremely sensitive documents, such as storing only on [air gapped](#) computers, disconnected storage devices or, for highly [sensitive information](#), in [hard copy](#) form only.

Integrity

[Integrity](#) involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people (for example, in a breach of confidentiality). These measures include file permissions and user [access controls](#). Version control may be used to prevent erroneous changes or accidental deletion by authorized users from becoming a problem. In addition, some means must be in place to detect any changes in data that might occur as a result of non-human-caused events such as an electromagnetic pulse ([EMP](#)) or server [crash](#). Some data might include [checksums](#), even [cryptographic checksums](#), for verification of integrity. [Backups](#) or redundancies must be available to restore the affected data to its correct state.

Availability

Availability is best ensured by rigorously maintaining all [hardware](#), performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment that is free of software conflicts. It's also important to keep current with all necessary system [upgrades](#). Providing adequate communication [bandwidth](#) and preventing the occurrence of [bottlenecks](#) are equally important. [Redundancy](#), [failover](#), [RAID](#) even [high-availability clusters](#) can mitigate serious consequences when hardware issues do occur.

Fast and adaptive [disaster recovery](#) is essential for the worst-case scenarios; that capacity is reliant on the existence of a comprehensive disaster recovery plan ([DRP](#)). Safeguards

against data loss or interruptions in connections must include unpredictable events such as natural disasters and fire. To prevent data loss from such occurrences, a [backup](#) copy may be stored in a geographically-isolated location, perhaps even in a fireproof, waterproof safe. Extra security equipment or software such as firewalls and proxy servers can guard against downtime and unreachable data blocked by malicious denial-of-service ([DoS](#)) attacks and network intrusions.

Special challenges for the CIA triad

[Big data](#) poses extra challenges to the CIA paradigm because of the sheer volume of information that needs to be safeguarded, the multiplicity of sources it comes from and the variety of formats in which it exists. Duplicate data sets and disaster recovery plans can multiply the already high costs. Furthermore, because the main concern of big data is collecting and making some kind of useful interpretation of all this information, responsible data oversight is often lacking. [Whistleblower](#) Edward Snowden brought that problem to the public forum when he reported on the NSA's collection of massive volumes of American citizens' personal data.

[Internet of Things privacy](#) is the special considerations required to protect the information of individuals from exposure in the [IoT](#) environment, in which almost any physical or logical entity or object can be given a [unique identifier](#) and the ability to communicate autonomously over the Internet or a similar network. The data transmitted by a given endpoint might not cause any privacy issues on its own. However, when even fragmented data from multiple endpoints is gathered, collated and analyzed, it can yield sensitive information.

[Internet of Things security](#) is also a special challenge because the IoT consists of so many Internet-enabled devices other than computers, which often go unpatched and are often configured with default or weak passwords. Unless adequately protected, IoT [things](#) could be used as separate attack vectors or part of a [thingbot](#). In a recent proof-of-concept exploit, for example, researchers demonstrated that a network could be compromised through a Wi-Fi-enabled light bulb. In December 2013, a researcher at Proofpoint, an enterprise security firm, discovered that hundreds of thousands of spam emails were being logged through a security gateway. Proofpoint traced the attacks to a botnet made up of 100,000 hacked appliances. As more and more products developed with the capacity to be networked, it's important to routinely consider security in product development.

Best practices in implementation

In implementing the CIA triad, an organization should follow a general set of best practices. Some best practices, divided by each of the three subjects, include:

Confidentiality

- Data should be handled based on their required privacy.
- Data should be encrypted, with a form of two-factor authentication to reach it.
- Keep access control lists and other file permissions up to date.

Integrity

- Ensure employees are knowledgeable about compliance and regulatory requirements.
- Use a backup and recovery software.
- To Ensure integrity, make use of version control, access control, data logs and checksums.

Availability

- Use preventative measures such as redundancy, failover and RAID. Ensure systems and applications stay updated.
- Use network or server monitoring systems.
- In case of data loss, ensure a Data Recovery and Business Continuity plan is in place.

History

The concept of the CIA triad formed over time and doesn't have a single creator. Confidentiality may have been first proposed as early as 1976 in a study by the U.S. Air Force. Likewise, the concept of integrity was explored in a 1987 paper titled "A Comparison of Commercial and Military Computer Security Policies." The paper recognized that commercial computing had a need for accounting records and data correctness. Even though it's not as easy to find an initial source, the concept of availability became more widespread one year later in 1988. By 1998 people saw the three concepts together as the CIA triad.