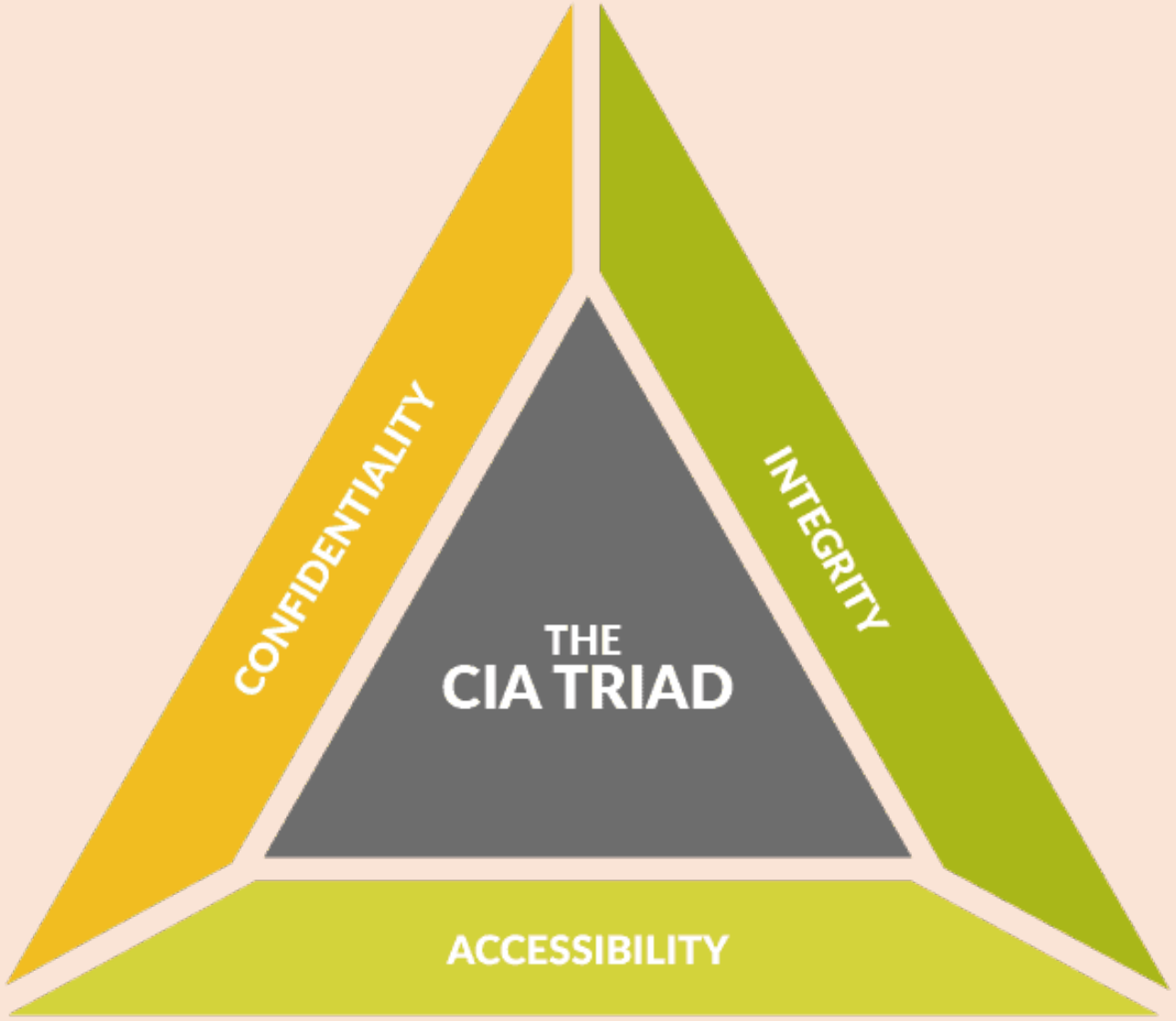
THE CIA TRIAD

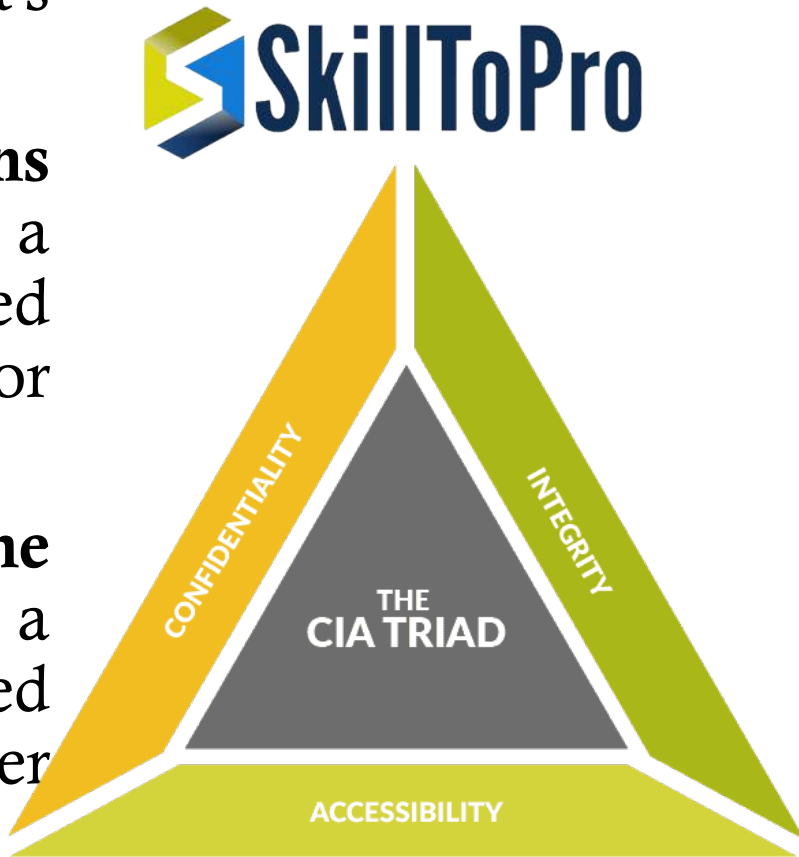
SkillToPro



THE CIA TRIAD- Cybersecurity Objective

The CIA Triad is a foundational principle in information security, outlining the three key objectives:

- **Confidentiality:** This ensures only **authorized individuals can access sensitive information**. Imagine it like a locked door; only those with the key (permission) can see what's inside.
- **Integrity:** This guarantees that **information remains accurate, complete, and unaltered.** Think of it like a document with a tamper-proof seal; any unauthorized changes would be obvious, preventing manipulation or corruption.
- **Availability:** This means **authorized users can access the information they need when they need it.** Picture it like a library with open doors and accessible books; authorized users can freely read and retrieve information whenever needed.



Here are some real-life examples:

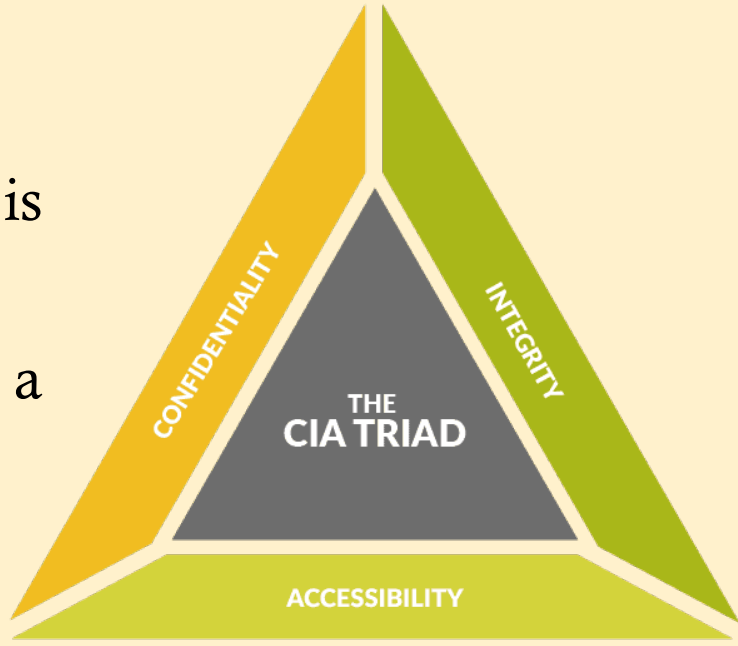
- **Confidentiality:** Protecting your social security number with encryption.
- **Integrity:** Using digital signatures to ensure documents haven't been tampered with.
- **Availability:** Having backups and disaster recovery plans to ensure systems are operational even after an outage.

Remember, these three elements work together:

- If information is confidential but not available, it's useless.
- If information is available but not accurate, it can be misleading.
- If information is accurate but accessible to anyone, privacy is compromised.

By aiming to achieve all three aspects of the CIA Triad, you can build a robust information security posture and protect your valuable data.

SkillToPro



CONFIDENTIALITY RISK

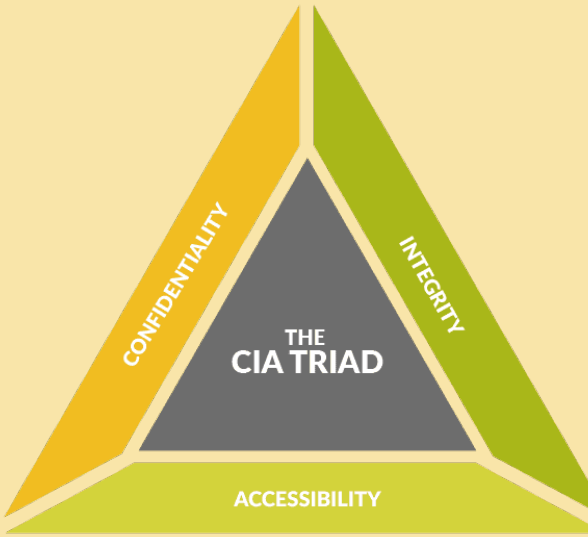
Snooping: Snooping is exactly what the name implies. The individual engaging in snooping wanders around your office or other facility and simply looks to see what information they can gather. When people leave sensitive papers on their desks or in a public area, it creates an opportunity for snooping.

Mitigant: By enforcing a clean desk policy. Employees should maintain a clean workspace and put away any sensitive materials whenever they step away, even if it's just for a moment.

Dumpster Diving: Dumpster diving attacks also look for sensitive materials, but the attacker doesn't walk around the office; instead, they look through the trash, trying to find sensitive documents that an employee threw in the garbage or recycling bin.

Mitigant: protect your organization against dumpster diving attacks using a simple piece of technology: a paper shredder! If you destroy documents before discarding them, you'll protect against a dumpster diver pulling them out of the trash.

SkillToPro



CONFIDENTIALITY RISK

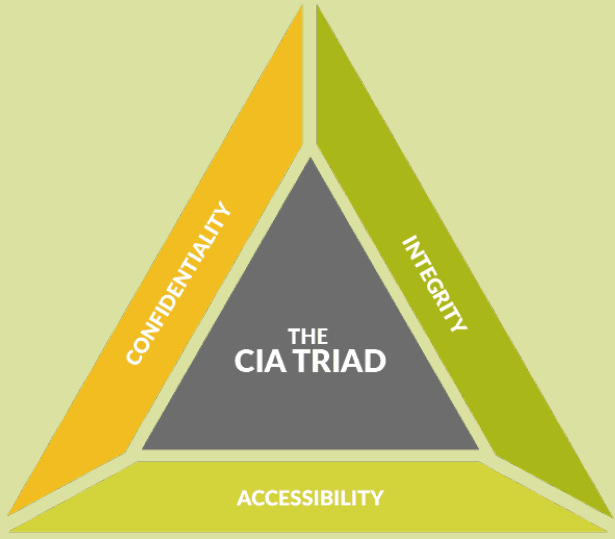
Eavesdropping: Eavesdropping attacks come in both physical and electronic types. In a physical eavesdropping attack, the attacker simply positions themselves where they can overhear conversations, such as in a cafeteria or hallway, and then listens for sensitive information.

Mitigant: You can protect against eavesdropping attacks by putting rules in place limiting where sensitive conversations may take place. For example, sensitive conversations should generally take place in a closed office or conference room.

Electronic eavesdropping attacks are also known as wiretapping. They occur when an attacker gains access to a network and monitors the data being sent electronically within an office.

The best way to protect against electronic eavesdropping attacks is to use encryption to protect information being sent over the network. If data is encrypted, an attacker who intercepts that data won't be able to make any sense of it. I'll talk more about how encryption works later.

SkillToPro

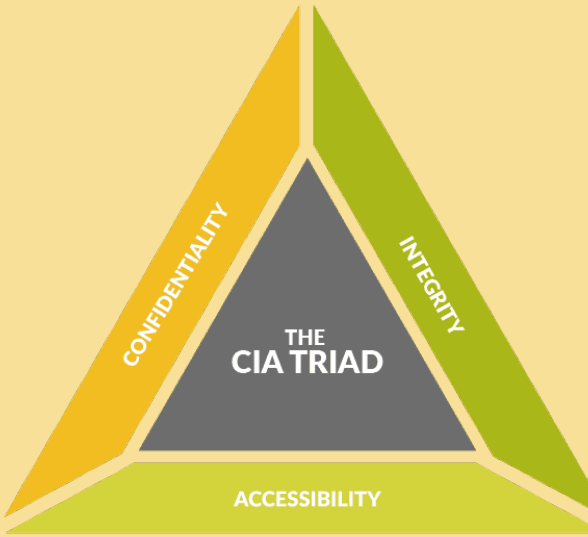


CONFIDENTIALITY RISK

Social Engineering: The last type of confidentiality attack I'll talk about is social engineering. In a social engineering attack, the attacker uses psychological tricks to persuade an employee to give them sensitive information or access to internal systems. They might pretend that they're on an urgent assignment from a senior leader, impersonate an IT technician, or send a phishing email.

Mitigant: It's difficult to protect against social engineering attacks. The best defense against these attacks is educating users to recognize the dangers of social engineering and empower them to intervene when they suspect an attack is taking place.

SkillToPro



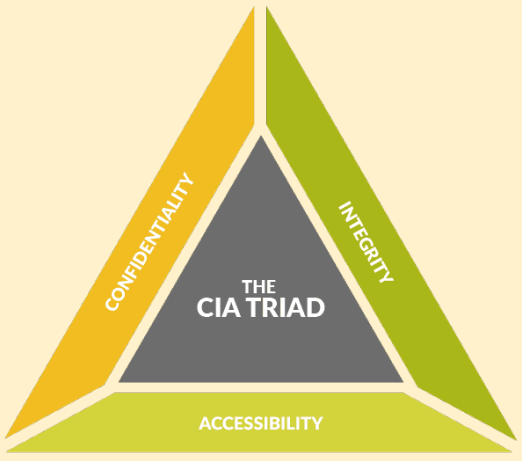
INTEGRITY RISK

Unauthorized Modification of Information: The ***unauthorized modification of information*** occurs when an attacker gains access to a system and makes changes that violate a security policy. This might be an external attack, such as an intruder breaking into a financial system and issuing themselves checks, or it might be an internal attack, such as an employee increasing their own salary in the payroll system.

Mitigant: Following the principle of ***least privilege*** is the best way to protect against integrity attacks. Organizations should carefully consider the permissions that each employee needs to perform their job and then limit employees to the smallest set of permissions possible.

Impersonation: In an ***impersonation attack***, the attacker pretends to be someone other than who they actually are. They might impersonate a manager, executive, or IT technician in order to convince someone to change data in a system. This is an extension of the social engineering attacks mentioned earlier.

Mitigant: the best defense against these attacks is **strong user education**.

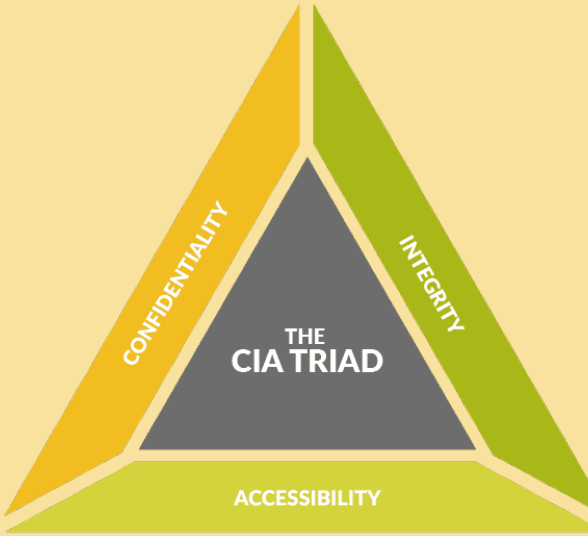


INTEGRITY RISK

Snooping: ***Man-in-the-Middle Attacks*** Sometimes impersonation attacks are electronic. In a man-in-the-middle (MitM) attack, the attacker intercepts network traffic as a user is logging into a system and pretends to be that system. They then sit in the middle of the communication, relaying information between the user and the system while they monitor everything that is occurring. In this type of attack, the attacker might be able to steal a user's password and use it later to log in to the system themselves.

Mitigant: By enforcing continuous network monitoring and detection tool. Implementation data encryption.

SkillToPro

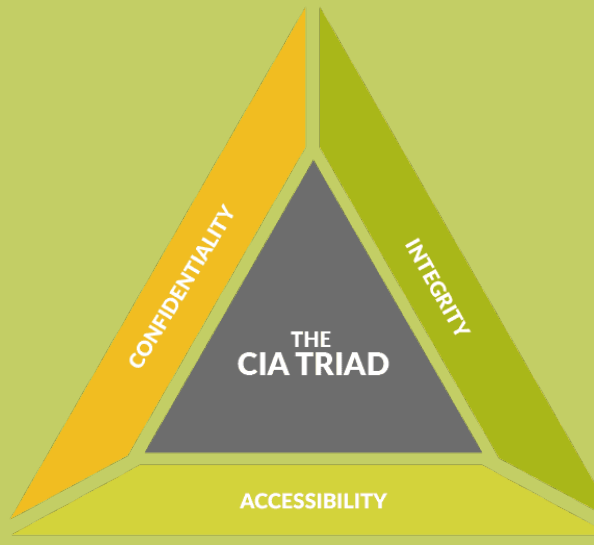


INTEGRITY RISK

Replay Attacks: In a replay attack, the attacker doesn't get in the middle of the communication but finds a way to observe a legitimate user logging into a system. They then capture the information used to log in to the system and later replay it on the network to gain access themselves.

Mitigant: The best defense against both replay and MitM attacks is the use of encryption to protect communications. For example, web traffic might use the Transport Layer Security (TLS) protocol to prevent an eavesdropper from observing network traffic. You'll learn more about this technology in Encryption.

SkillToPro

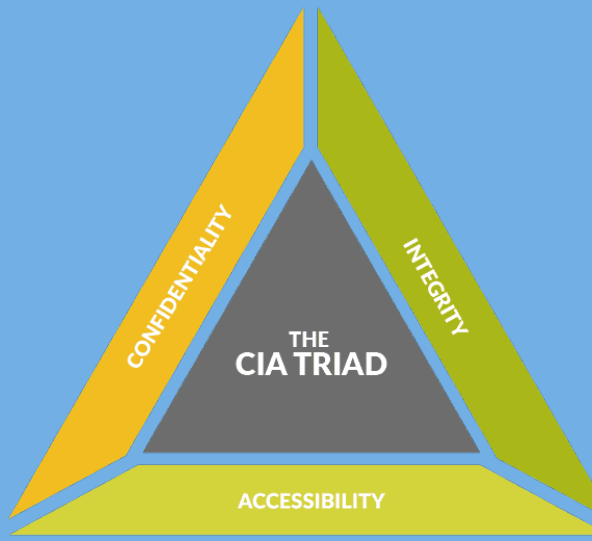


AVAILABILITY RISKS

Denial-of-Service Attacks: Denial-of-service (DoS) attacks occur when a malicious individual bombards a system with an overwhelming amount of network traffic. The idea is to simply send so many requests to a server that it is unable to answer any requests from legitimate users.

Mitigant: You can protect your systems against DoS attacks by using firewalls that block illegitimate requests and by partnering with your Internet service provider to block DoS attacks before they reach your network.

SkillToPro



AVAILABILITY RISKS

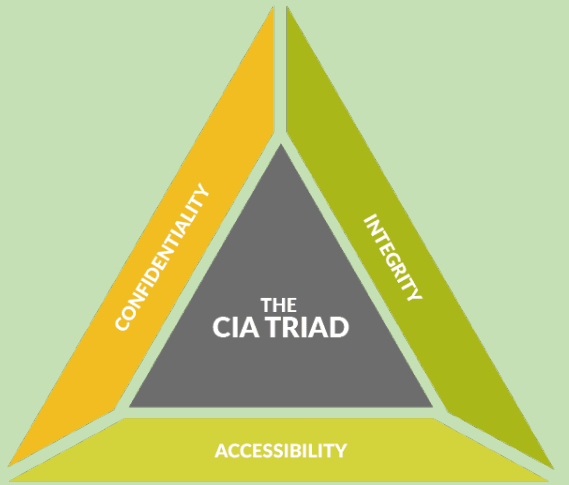
Power Outages: Power outages can occur on a local or regional level for many different reasons. Increased demand can overwhelm the power grid; natural disasters can disrupt service; and other factors can cause power outages that disrupt access to systems.

Mitigant: You can protect against power outages by having redundant power sources and backup generators that supply power to your system when commercial power is not available.

Hardware Failures: Hardware failures can and do occur. Servers, hard drives, network gear, and other equipment all fail occasionally and can disrupt access to information. That's an availability problem.

Mitigant: You can protect against hardware failures by building a system that has built-in redundancy so that if one component fails, another is ready to pick up the slack.

SkillToPro



AVAILABILITY RISKS

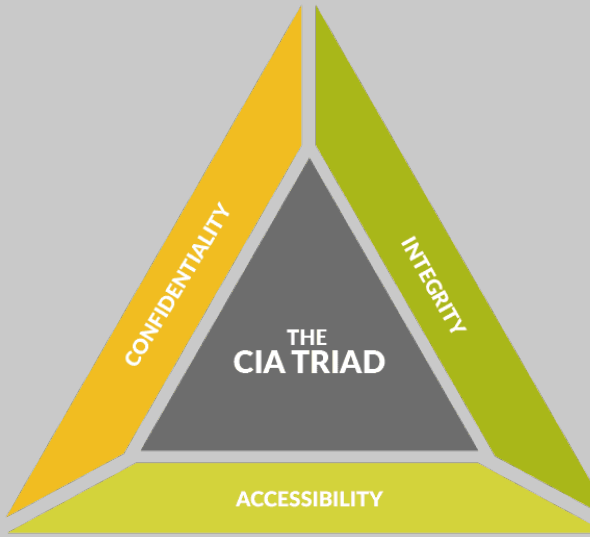
Destruction of Equipment: Sometimes equipment is just outright destroyed. This might be the result of intentional or accidental physical damage, or it may be the result of a larger disaster, such as a fire or a hurricane.

Mitigant: You can protect against small-scale destruction with redundant systems. If you want to protect against larger-scale disasters, you may need to have backup data centers in remote locations or in the cloud that can keep

Service Outages: Sometimes service outages occur. This might be due to programming errors, the failure of underlying equipment, or many other reasons. These outages disrupt user access to systems and information and are, therefore, an availability concern.

Mitigant: You can protect against service outages by building systems that are resilient in the face of errors and hardware failures.

SkillToPro



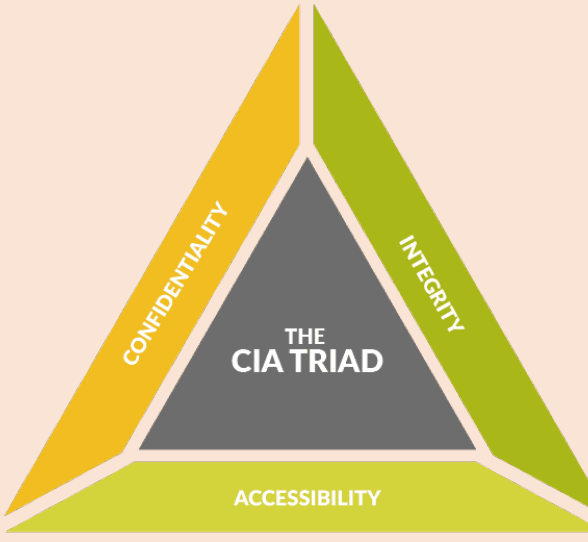
NON-REPUDIATION

Non-repudiation is a security concept that ensures that ***someone cannot deny*** performing an action or being the author of a piece of data. It's like a ***digital fingerprint*** that proves someone was involved in something, without a doubt.

Here are some of the key aspects of non-repudiation:

- **Origin:** It guarantees that the data or action originated from a specific individual or entity.
- **Integrity:** It verifies that the data or action hasn't been tampered with after it was created.
- **Delivery:** It confirms that the data or action was delivered to the intended recipient.

SkillToPro

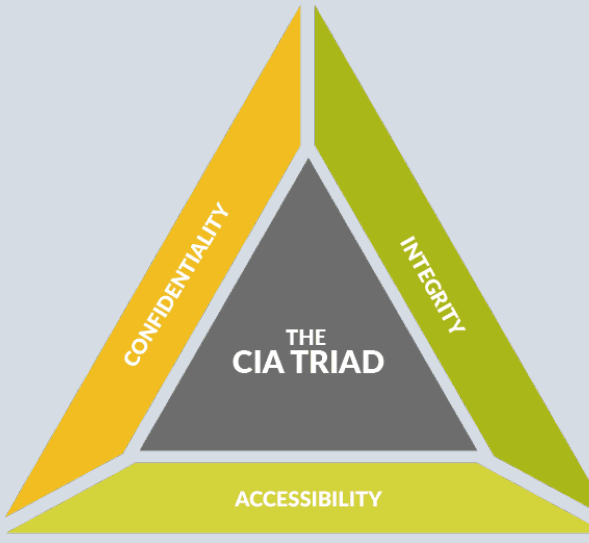


NON-REPUDIATION

Non-repudiation is crucial in various situations, such as:

- **Electronic contracts:** It ensures that both parties involved in a contract cannot deny signing it.
- **Financial transactions:** It prevents fraud by verifying the identity of the sender and recipient of funds.
- **Medical records:** It protects patient privacy by ensuring that only authorized individuals can access their medical information.
- **Voting systems:** It safeguards the integrity of elections by preventing unauthorized individuals from voting or tampering with votes.

SkillToPro

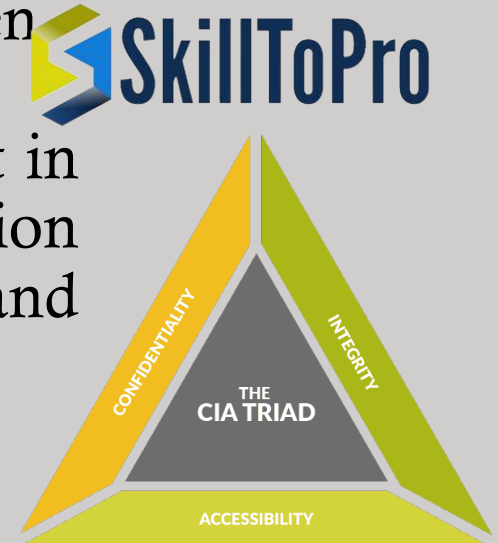


NON-REPUDIATION

There are several technologies that can be used to achieve non-repudiation, including:

- **Digital signatures:** These are electronic signatures that are created using cryptography. They provide a way to verify the identity of the signer and ensure that the data has not been tampered with.
- **Timestamping services:** These services provide a secure way to record the time and date that a piece of data was created. This can be used to prove when someone performed an action.
- **Secure audit logs:** These logs track all activity that takes place on a system. They can be used to identify who performed an action and when.

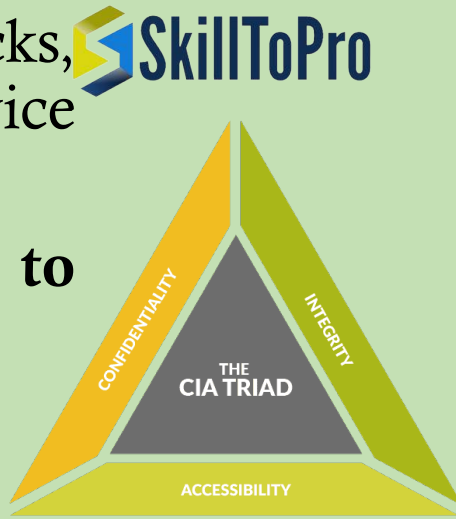
Non-repudiation is an essential security principle that helps to build trust in electronic transactions and communications. By using non-repudiation technologies, organizations can protect themselves from fraud, errors, and unauthorized access.



EXAM HINTS

The CIA triad references the three main goals of information security: confidentiality, integrity, and availability.

- Confidentiality protects sensitive information from **unauthorized access**. The major threats to confidentiality include snooping, dumpster diving, eavesdropping, wiretapping, and social engineering.
- Integrity protects information and systems from **unauthorized modification**. The major threats to integrity include the unauthorized modification of information, impersonation attacks, man-in-the-middle attacks, and replay attacks.
- Availability ensures **that authorized users have access to information** when they need it. The major threats to availability include denial-of-service attacks, power outages, hardware failures, destruction of equipment, and service outages.
- Non-repudiation uses technical measures to ensure that a user is **not able to later deny** that they took some action.



5 pillars of information assurance

Availability	Integrity	Authentication	Confidentiality	Nonrepudiation
Ensures information is ready for use and at the required performance level.	Guarantees data, associated systems only accessible or modifiable by authorized users.	Ensures users are who they say they are (i.e., user names/passwords, biometrics, digital certificates and security tokens).	Limits access or places restrictions on data like personally identifiable information/ classified corporate data.	Ensures individuals cannot deny an action because a system provides proof of the action.