# **CompTIA Security+**

**Four Control Categories**

**Technical Controls**

* Controls implemented using system.
* Operating system controls
* Firewalls, anti-virus

**Managerial Controls**

* Administrative controls associated with security design and implementation
* Security policies, standard operating procedures

**Operational Controls**

* Controls implemented by people instead of systems
* Security guards, awareness programs

**Physical Controls**

* Would limit physical access like;
* Guard shack
* Fences, locks
* Badge readers

**Control Types**

**Preventive Control** – Block access to a resource

**Deterrent Control** – Discourage an intrusion attempt. Not directly preventing access.

**Detective Control** – Identify and log an intrusion attempt, may not prevent, but still provide a warning and a log.

**Corrective Control** – Apply a control after an event has been detected. To reverse the impact of an event.

**Compensating Control** – using other means to control, specially when the controls aren’t sufficient and may be temporary.

**Directive Control** – directing a subject or someone to do something to make something more secure. Security compliance.

*Note: Some organizations may combine types of controls.*

**THE CIA Triad**

* Combination of Principles (Fundamentals of Security)
* Sometimes referenced as AIC Triad

**Confidentiality** – Prevent disclosure of information to unauthorized individuals or systems.

-use ***Encryption***to encodes messages so only certain people can read it.

- use ***Access Controls***to select people or restrict access to a resource.

- use ***Two-factor Authentication*** to have an additional confirmation before information disclosed.

**Integrity** – Sending an information making sure the messages cannot be modified without detection

-***Hashing*** to map data of an arbitrary length to data of a fixed length

-***Digital signatures*** is a mathematical scheme to verify the integrity of data.

-***Certificates*** combine with digital signature to verify an individual.

-***Non-repudiation*** provides proof of integrity, can be asserted to be genuine.

**Availability** – Systems and network must be up and running.

-***Redundancy*** build services that will always be available

­-***Fault Tolerance*** system will continue to run, even when a failure occurs

-***Patching*** ensures stability and closes security holes or exploits.

**NON-REPUDIATION**

**Proof of Integrity** – Verify data does not change. Data is accurate and consistent.

We use *hash/hashing* in cryptography. Wherein we represent data as a short string of text.

If the data changes, the hash changes.

Doesn’t necessarily associate data with an individual. It only tells if the data has changed.

**Proof of Origin** – prove the message was not changed (Integrity)

-Prove the source of the message (Authentication)

-Make sure the signature is not fake (Non-repudiation)

-Sign with the private key, wherein nobody else can sign.

-verify with public key. Any change to the message will invalidate the signature.