

## Unit 1: Network and Information Security Management: History & Definitions

In week one (1) studies, I revised the CIA triad definition and learned non-repudiation as an extension to the triad. When I studied CISSP, it was a component of the controls with Accountability depending on non-repudiation. Other concepts that I learned are vulnerabilities, threats, threat agents and exploit.



CIA+N TENETS	Goal	Examples	Threats
Confidentiality	Prevents unauthorised disclosure of information and unauthorised access to data.	Encryption and Authentication.	Theft of PII, packet capturing and social engineering.
Integrity	Prevents unauthorised modification of data and unauthorised write access to data.	Permission control, audit logs and checksums.	Session hijacking and man-in-the-middle attack.
Availability	Systems and information are available timeously when needed.	High-Availability configuration, site resiliency and backups.	DoS-Denial of Service, ICMP flood and electrical power blackout.
Non-Repudiation	Ensures Accountability of actions performed.	Authentication, Accountability(logging) and Integrity.	Malware and forgery.

Furthermore, I learned components of the Information Security Management System (ISMS).

