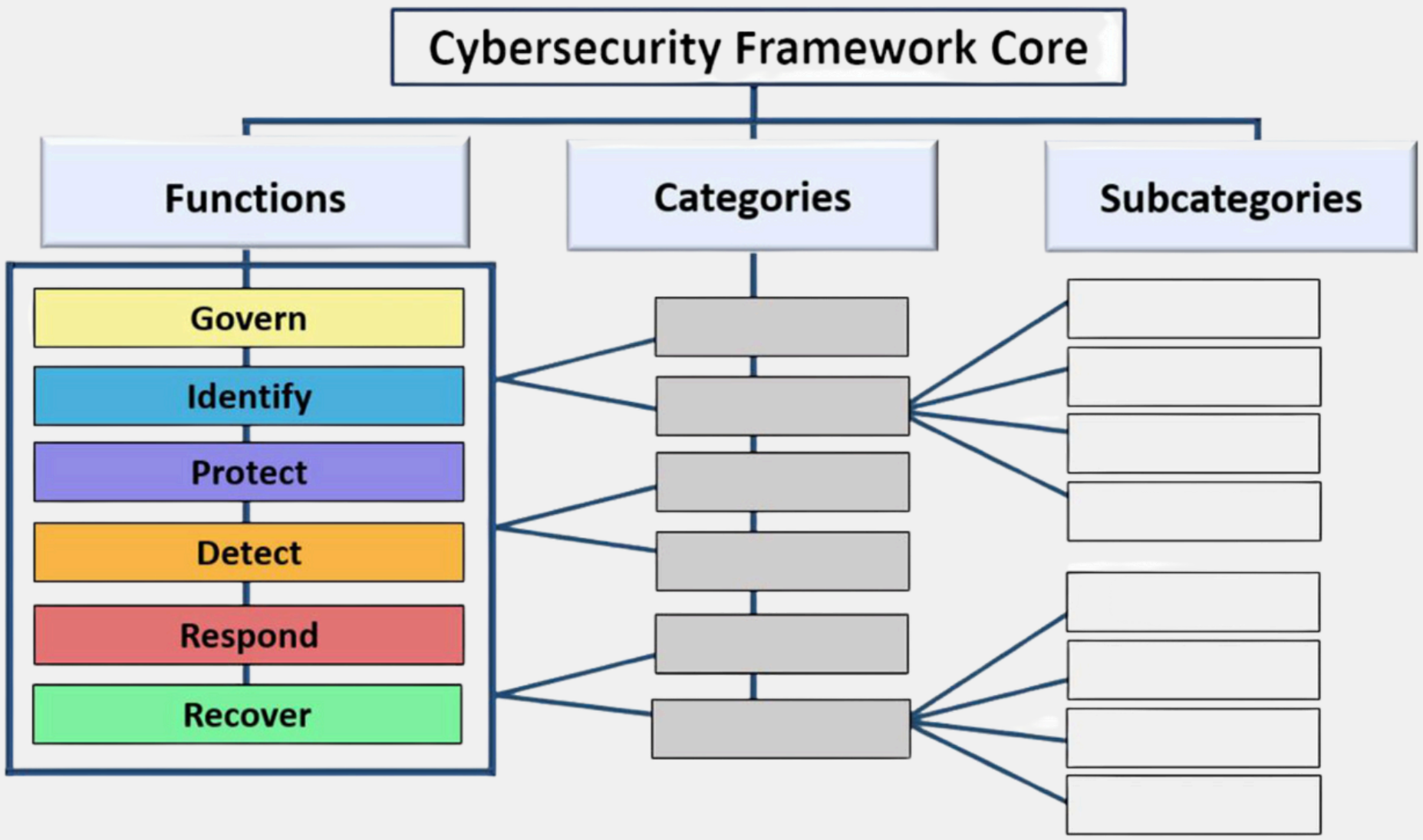
Aron Lange

@LangeAron

NIST Cybersecurity Framework 2.0



131 Retweets **1.3K** Likes

Aron Lange

@LangeAron

Cybersecurity Framework **Core**

6
FUNCTIONS

22
Categories

106
Subcategories

131 Retweets **1.3K** Likes

Aron Lange

@LangeAron

Cybersecurity Framework **Functions**

Govern (GV)	The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.
Identify (ID)	The organization's current cybersecurity risks are understood.
Protect (PR)	Safeguards to manage the organization's cybersecurity risks are used.
Detect (DE)	Possible cybersecurity attacks and compromises are found and analyzed.
Respond (RS)	Actions regarding a detected cybersecurity incident are taken.
Recover (RC)	Assets and operations affected by a cybersecurity incident are restored.

131 Retweets **1.3K** Likes

Aron Lange

@LangeAron

Cybersecurity Framework **Core**

131 Retweets **1.3K** Likes

Aron Lange 

@LangeAron

Functions are supported by **Categories**

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Aron Lange

@LangeAron

Subcategories further divide Categories

IDENTIFY (ID): The organization's current cybersecurity risks are understood

- **Asset Management (ID.AM):** Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy
  - **ID.AM-01:** Inventories of hardware managed by the organization are maintained
  - **ID.AM-02:** Inventories of software, services, and systems managed by the organization are maintained
  - **ID.AM-03:** Representations of the organization's authorized network communication and internal and external network data flows are maintained
  - **ID.AM-04:** Inventories of services provided by suppliers are maintained
  - **ID.AM-05:** Assets are prioritized based on classification, criticality, resources, and impact on the mission
  - **ID.AM-07:** Inventories of data and corresponding metadata for designated data types are maintained
  - **ID.AM-08:** Systems, hardware, software, services, and data are managed throughout their life cycles