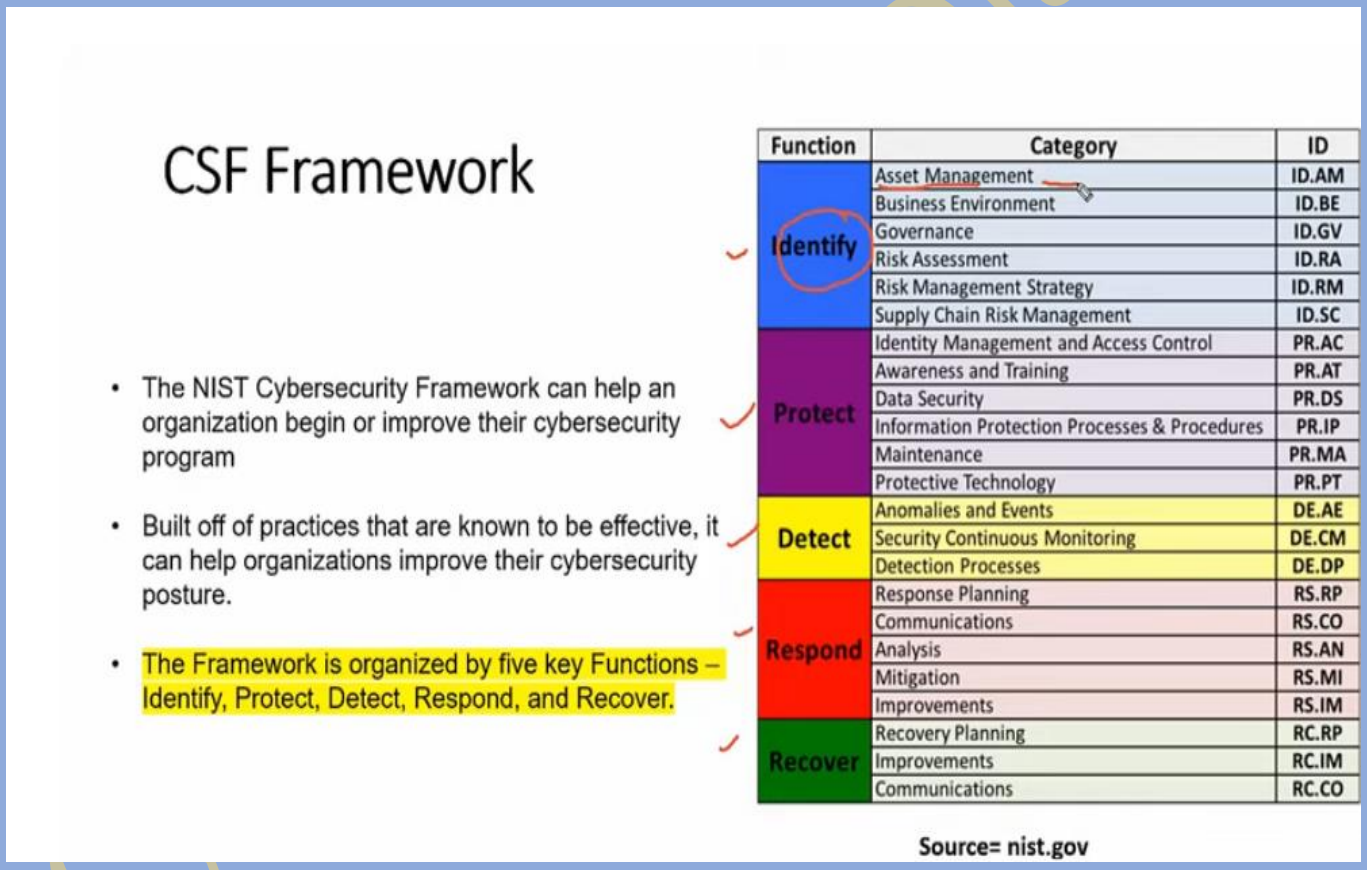
Introduction to NIST CSF Framework

The NIST framework can help the organization to build and improve cyber security posture

It consists of five main functions (IPDRR):

- Identify
- Protect
- Detect
- Respond
- Recover



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

We have different audience who perceive cyber security frameworks differently:

- ***Executives:*** They want to understand the responsibility roles
- ***IT management:*** The business impact
- ***Legal Team:*** wants to know the threats in the legal aspect
- ***Implementers:*** How to implement controls

Building a Cyber Security Posture

Step 0: Collecting Information

- Organization blue print: chart, objectives, CISO, critical data, critical process
- Organization vision and mission
- Organization business plan: meeting, revenue expectation,
- Current information security governance: ISMS posture

Step 1: Prioritize scope

- Identify the executives
- Define the scope for CSF application CSF
- Determine the risk appetite
- Identify the systems
- Vision, missions, directives - Funding

Step 2: Orient

We get information about:

- Threats
- Service agreements
- Availability
- Risk assessment
- Current profiles

Step 3: Create Current profile

- What are the current threats?
- Which vulnerabilities do we have?
- What cyber security maturity do we have?
- We need to document what is the desired state

Step 4: Conduct the risk Assessment

- Assets need to be classified based on criticality, impact of the business
- We document the vulnerabilities, the risk registers
- What we get here is the catalogue of potential risk events, target capabilities levels & profiles, Risk Assessment results

Step 5: Create a target profile

- Document the respective controls, categories, processes
- Prioritize what we need to implement first, which is done in the next step

Step 6: Determine, Analyze and Prioritize

- The organization performs the gap analysis to determine the opportunities for improvement
- The gaps are identified by overlaying the current state profile with the target state profile
- This step is very essential

Step 7: Implement action plan

- The required actions are taken to close the gap and obtain the target current state