NIST CYBERSECURITY FRAMEWORK 2.0 (CSF 2.0)
Core Functions Overview

The NIST CSF 2.0 is organized around six core Functions which provide a high-level view of the lifecycle of an organization's management of cybersecurity risk.

1. GOVERN (GV)
The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.
- GV.OC: Organizational Context - The circumstances — mission, stakeholder expectations, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood.
- GV.RM: Risk Management Strategy - The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established.

2. IDENTIFY (ID)
The organization's current cybersecurity risks are understood.
- ID.AM: Asset Management - Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed.
- ID.RA: Risk Assessment - The cybersecurity risks to the organization, assets, and individuals are understood.

3. PROTECT (PR)
Safeguards to manage the organization's cybersecurity risks are used.
- PR.AA: Identity Management, Authentication, and Access Control - Access to physical and logical assets is limited to authorized users, processes, and devices.
- PR.DS: Data Security - Data is managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

4. DETECT (DE)
Possible cybersecurity attacks and compromises are found and analyzed.
- DE.AE: Adverse Event Analysis - Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents.

5. RESPOND (RS)
Actions regarding a detected cybersecurity incident are taken.
- RS.MA: Incident Management - Responses to detected cybersecurity incidents are managed.

6. RECOVER (RC)
Assets and operations affected by a cybersecurity incident are restored.
- RC.RP: Incident Recovery Plan Execution - Recovery activities are performed according to the recovery plan.