NIST CSF 2.0 - Governance Function for Organizational Context

It ensures proper monitoring of the organization's cyber security posture: risk management, policies, strategies and controls

The function entails:

- Organizational Context
- Risk Management Strategy
- Cyber Security Supply Chain Management
- Roles, Responsibilities and Authorities
- Policies, processes and Procedure
- Oversight

Implementing The Organizational Context

1) Understanding Governance

i) Healthcare:

- Protect patient data
- Protect Intellectual Property

ii) Financial Services:

- Protection of customer data
- Implement secure access controls

iii) Government agencies:

- Protect their classified information
- Protect their critical IT infrastructure

2) Every organization has its own context

- Mission: why does the organization exist
- Objectives: specific, measurables goals: creativity, innovations
- Stakeholders: these are the interested parties
- Activities

3) Enhancing the organizational context

- By establishing communication priorities
- Ensure the alignment of the organization members
- Make informed decisions about the allocation of resources, especially cyber security resources
- Understand which assets are more critical to the organization's mission, vision; to allow effective management

4) Understand the vision and mission

- Vision: what the organization wants to be when it grows up
- Mission: what we are

5) Understand the business objectives

- Revenue and growth targets
- Market expansion's plan
- Product and service launches

6) Understand the organizational structure

- Centralized or decentralized
- Departments and their interdependencies

7) Regulatory Environment

- Industry specific (HIPPA, GDPR)
- Compliance requirements
- Audit and reporting obligations

8) Risk Appetite

- Tolerance of risk (high, medium, low)
- Business areas with high-risk exposure

9) Stakeholders

- Internal (employees, management, board)
- External (customers, partners, regulators)

10) Cultural aspects

- Organizational value and beliefs
- Attitude to innovation changes
- Employee awareness training

11) Technological landscape

- Existing IT infrastructure
- Adoption of new technologies
- Legacy systems and vulnerabilities

12) Financial considerations

- Budget allocated for information security
- Cost-benefit analysis of security investments

13) Incident History

- Past security breaches or incidents
- Lessons learned and corrective actions taken

NIST Requirement

- **GV. OC-01:** The organizational mission is understood and is informed to the risk management team
- **GV. OC-02:** Internal and external stakeholders are determined and their needs regarding cyber security risk management are understood

- **GV. OC-03:** Legal regulatory and contractual requirements regarding cyber security - are understood and managed
- **GV. OC-04:** Critical objectives, capabilities that stakeholders depend on or expect from the organization are determined and communicated
- **GV. OC-05:** outcomes, capabilities and services that the organization depends on are determined and communicated

Documentation Requirements

- Mission and vision documentation
- Type of industry you work
- List of legal and regulatory requirements (process to work)
- List of Services and products offer
- Any certification the organization achieved
- Business requirement documentation sign off
- Inventory of policies
- Information security strategy align with business requirement
- Organization chart and reporting matrix
- Any legal officer or counsel
- Inventory of critical services (internal and external)