NIST CSF - Identify Function for Asset Management

In any organization we need to identify what we have and what we need to protect:

- Physical devices and systems within the organization must be inventoried
- Software platforms and applications within the organization are inventoried
- Communication data flaw should be mapped
- External information is catalogued
- Resources must be organized

CSF Function ID - Identify

- In order to identify something, we need visibility
- The organization should protect the resources, data, processes and capabilities, compliance requirements
- This will help the organization to determine the threats and vulnerabilities
- Understanding the business context, the resources that support critical functions and the related cyber security risks enable an organization to focus and prioritize its efforts and also be consistent with its risk management strategy and business needs

Categories:

- ID. AM - Asset Management
- ID. BE - Business Environment
- ID. GV - Governance
- ID.RA - Risk Assessment
- ID. RM -Risk Management Strategy
- ID. SC - Supply Chain Risk Management

Asset Management:

1) **Physical devices and systems within the organization are inventoried:**

- In the organization according to ISO 27001 the first thing it to ensure that there is a solid asset inventory and NIST CSF still requires the same
- The organization should have the full understanding of the assets (Resources) and if they have a control
- They need to understand the vulnerabilities of each asset

- They need to understand the associate risk and impact of the vulnerabilities on the business
- It is vital to know which assets are critical and need to be prioritized for protection
- Network all the hardware, network infrastructure, physical machines
- If there is no cyber security in that organization, first schedule a meeting with the owner of the organization and understand the vision and mission of that organization
- Document all the assets to know which one supports the organization

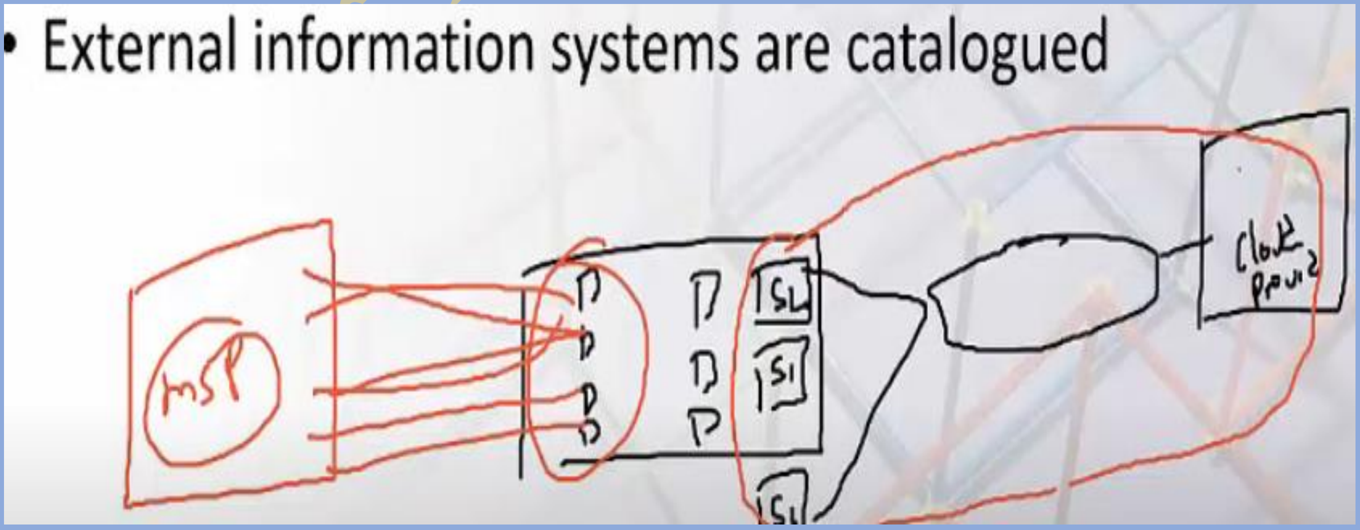
2) Software platforms and applications within the organization are inventoried:

- Device >>>> Applications running
- Approved list of softwares shall be maintained by the IT department
- Any request for the software installation that is not included in the approved software release should be removed or require approval from the Chief Information Officer
- You need to maintain a list of all assets, to provide ownership of softwares

3) Organizational Communications and data flows are mapped:

- Questionnaires
- Email system encryption
- Review and update formal document of risk assessment
- Data classification system

4) External systems are catalogued:



- External information systems are catalogued

5) **Resources e.g. Hardware, devices, time personnel and software) are prioritized based on their classification criticality and business value**

6) **Cyber Security roles and responsibility for the entire workforce and third-party stakeholders (e.g. suppliers, customers & partners) are established**