Framework for Improving Critical Infrastructure Cybersecurity

The goal of the NIST is to identify and mitigate the risks, of Cybersecurity threats to the critical infrastructure of the United States. NIST goal is to create an environment in the world of cyber threat, whereby efficiency; innovation and the economy can prosper. In order to achieve this goal a set of industry standards and best practices have been established also called as the Cyber Security Framework. The goal of the Framework is to use the have business consider cybersecurity risks as part of the organizations risk management process.

The Framework consist of three parts: The Frame core, the Framework Profile, and the Framework Implementation Tiers. Though they are separately defined they are also interrelated because, the Framework Core consist of information and outcomes which provides guidelines for developing individual profiles, based on the common core every infrastructure develops its individual profile/needs. Through use of the Profiles, the Framework will help the organization align its cybersecurity activities with its business requirements, risk tolerances, and resources. Having developed the profiles implementation Tiers are used as a mechanism for Organizations to view and understand the characteristics of their approach to managing Cybersecurity risk.

- Framework Core: Main objective is to allow a channel of communication pertaining to cybersecurity activities and its outcomes across all levels of the organization, from top to bottom. The core is made up of four elements mainly, Functions organize activities at the highest level, which functions will be divided in to categories tied to the needs and particular activities, further subcategories are created of the categories based on specific outcomes and finally assign standards and guidelines for achievement of each sub categories, which are required to work together with the help of five concurrent and continuous functions like Identify, Protect, Detect, Respond and Recover

- Framework Implantation: Provides answer to risks perceived cybersecurity risks by the organization and how it plans to manage that risk by having Tiered processes in place. The Tiers are divided into 4 types as:

    - Tier 1: which is partial (response to security threat). The risk in this tier is that the cyber security risk managed without total awareness and the response will be ad hoc and reactive. This tier is broadly categorized into three subcategories as per the above responses namely a- Risk Management Process, b- Integrated Risk Management Program and c- External Participation.
    - Tier 2 :(The framework Implementation tier) is broadly divided into three subcategories a- Risk Management Process, b- Integrated Risk Management Program and External Participation. The response to cyber threat provided by this tier is based on the management's awareness of cybersecurity risks and at the same rime risk management processes are approved by the management however an Organization-wide approach to managing cybersecurity risk has not been established or communicated and shared within the organization.

- Tier 3: (Repeatable) is also subdivided in to three responses levels. a- Risk Management Process, b- Integrated Risk Management Process and c- External Participation. Under this tier the Organizations cybersecurity risk management practices are formally approved and procedure are defined, implementation as intended and reviewed.
- Tier 4: (Adaptive) is also subdivided in to three response levels. a- Risk management process, b- Integrated Risk Management Program and c- External Participation. Under this tier the Organizations response is based on the learning process from previous responses and improvements are shared by other sources.

- Framework Profile: Under this profile the organization aligns its Functions, categories, and Subcategories with the business requirements, risk tolerances, and resources of the organizations.