**Understanding the NIST Cybersecurity Framework**

Data is the most valuable asset which is the reason why data security has taken over a huge agenda. Data breaching and security failures can put the world to risk. Realizing the importance of data security worldwide, the President of the United States issued an executive order to develop a cybersecurity framework to mitigate the risk of cyber-attacks. These are a set of rules and guidelines that help organizations to improve their cybersecurity architecture.

**Types Of Frameworks**

The first type of network is called PCI-DSS, which stands for Payment Card Industry and Data Security Standards which is designed to protect debit card, credit card, and cash card transactions.

The second type of framework is ISO 27001/27002 which recommends best practices for information security management and program elements are given by this.

The third type is the CIS, which stands for Critical Security Controls framework. This gives cyber protection by giving noteworthy approaches to the present attacks.

The last type is NIST frameworks which are made for improving critical infrastructure cybersecurity to improve organizations' risks by leveraging standard methodologies and processes.

**What is the NIST framework?**

This is nothing but voluntary guidance that is based on existing standards guidelines, and practices for organizations to better manage and mitigate the cybersecurity risks. In addition to helping organizations manage and reduce risk, it was designed to foster risk and cybersecurity communications among both internal and external organizational stakeholders. This framework is drafted by the National Institute of Standards And Technology (NIST). Whether we are initiating a cybersecurity program or already running a program, this framework gives us value and acts as a management tool to mitigate the risks.

**The need for this framework**

The purpose of the framework is to understand, manage and reduce its cybersecurity risks. It will help in figuring out which activities have prior importance to assure critical operations. In turn, it will help prioritize investments and maximize the impact of each dollar spent on cybersecurity.

1) It results in a shift of compliance to action and specifies outcomes by providing a common language to address cyber security risk management, especially helpful in communicating inside and outside the organization including improving communication and awareness among IT planning and operating units as well as senior executives of organizations.

2) It gives us a measure of where we are and where we have to go.

3)It can be implemented in stages or degrees which makes it more appealing.

4) It has a built-in maturity model and gap analysis so we don’t need an additional maturity model on top of CSF. Organizations can also readily use the framework to communicate current or desired Cybersecurity postures.

**References**

1)<https://www.balbix.com/insights/nist-cybersecurity-framework/>

2)<https://www.nist.gov/cyberframework>

3)<https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework>

4)<https://www.techtarget.com/searchsecurity/definition/NIST-Cybersecurity-Framework>

5)<https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework>

6)<https://www.ftptoday.com/what-is-nist>

7)<https://is.bryant.edu/files/36176381/36176467/1/1563546609000/implementing_nist_framework.pdf>