The National Institute of Standards and Technology (NIST) Cyber Security Framework(CSF) is all about providing procedures and details for improving and securing the critical cybersecurity infrastructure and the malicious cyber-attacks. Thus, selecting an appropriate cybersecurity framework is an important task for the organization which will have significant effects on the organization to overcome the risks and making the company secured on a large scale and having Policies and procedures less vulnerable to the confidentiality, security and availability of the information of the organization.

There are set of procedures and actions which a CSF personnel must follow as per the standards, at the higher level they are divided as follow:

**Identify:**This is a foundation phase where the effective use of the CSF is decided. This is the phase which identifies and defines the problems and the factors causing the problem.eg; Asset Management, governance, Risk assessment and management strategy.

**Protect:**This function defines the security measures or limits of the problem. eg; Training and awareness, Data security, Maintenance and protective technology.

**Detect:**In this phase, we detect the factors which cause the vulnerability of data to the outside world or occurrence of cybersecurity events. eg; Continuous Monitoring, detection process.

**Response:** Here we develop and implement the security measures and actions to overcome the cybersecurity events.eg; response planning, mitigation, Analysis, improvements and communications etc.

**Recover:**Appropriate recovery plans are laid out to restore the services that were affected the cybersecurity events.eg; Recovery planning, improvements.

Here we are going to discuss in detail the RESPONSE phase of the framework and what effect it has on improving and overcoming the problem faced by the organization.

Conducting the assessment in today's sophisticated information technology where the mission and vision of the organizations are very clear can be more difficult and challenging.

The response phase has the ability to control the effects of the potential cybersecurity events. The response function is directly related to the detect function. **Stronger the detect function stronger will be the response function**, as we can only respond to what we detect.  Below is the explanation of the main categories and the sub-categories of the response function which all the organization must follow while implementing CSF.

**1.Response planning:**They are set of procedures to follow in case event occurs. The aim of this plan is to respond immediately with no delay and corrective actions can be taken.

**a**. RS.RP: The response plan is executed during and after the event occurs.

**2**. **Communication**: It plays the main role while communicating the response activities to the internal and external stakeholders to get the appropriate support from law enforcement companies.

**a**. Everyone in the organization should know their role when the response is needed.

b. Events should be consistently reported with the newly added criteria.

c. Information is shared continuously to keep everyone updated about the events.

d. Communication helps coordinate with stakeholders easily with the response plan.

e. Volunteer exchange of information with stakeholders when they need a broader picture.

**3. Analysis:**A detailed analysis should be done to check if there are proper response and recovery actions taken to face the events when occurred.

a. Notifications from the detection systems should be monitored.

b. Understanding how big or small the impact can be.

c. Detailed analysis should be done to know the root cause of the event.

d. Properly categories the incident to fall under the proper response plan.

**4.Mitigation:**We should have the plan ready to stop the event from affecting the system any further and should resolve the action at the earliest possible way.

a. The incident should be identified.

b. The incident should be mitigated as early as possible.

c. New events should be documented and response plan should be laid out for future use.

**5.Improvements:**Improvement in the system and response plans can be implemented to overcome the similar issue in future.

a. All the documents in the framework must be updated.

b. Response plan to deal with the similar issue should be communicated internally and externally.

As a team member of the implementing the CSF team in an organization and specially assessing the response phase, I would like all the members to follow the above points to make the system less prone to the cyber-attack which can even prevent the organization in future attack and reduced the chances of malicious activities making the organization secure while dealing with confidential and secured information.