Checklist for Implementing NIST Cybersecurity Framework

The NIST Cybersecurity Framework (CSF) implementation requires multiple steps. Remember, you can always tailor these checklists to your organization's size and needs. The following checklist will help you adopt NIST CSF:

#1. Prepare and Organize

- Create a dedicated implementation team.
- Define your organization's implementation scope.
- Set defined NIST CSF implementation targets

#2. Understand your Current State

- Comprehensively examine your company's cybersecurity risk.
- Identify vital data, systems, and assets.
- Assess cybersecurity policies, processes, and controls

#3. Match Business Goals

- Align your business goals with the NIST CSF.
- Inform stakeholders of cybersecurity's relevance

#4. Function-NIST CSF Core Elements Mapping

- Learn the NIST CSF's five basic functions: Identify, Protect, Detect, Respond, and Recover.
- Connect cybersecurity activities to key functions.

#5. Create Current Profile

- Create a NIST CSF cybersecurity profile for your organization.
- Assess each key function's strengths and limitations

#6. Create a Target Profile

- ★ Choose a profile matching your company's cybersecurity goals.
- ★ Set explicit improvement targets and outcomes

#7. Set priorities and Implement Changes:

- ★ Use current and target profiles to prioritize improvements.
- ★ Create and implement a gap-and-vulnerability roadmap

#8. Implement NIST CSF Functions

- ★ Implement key functions, activities, and controls.
- ★ Customize implementation for your company's risks and needs

#9. Integrate Existing Processes

- ★ Make NIST CSF operations compatible with cybersecurity processes.
- ★ Apply the framework to daily tasks and decisions.

#10. Training and Awareness

- ★ Educate personnel on NIST CSF and its fundamental functions.
- ★ Increase awareness of individual cybersecurity contributions.

#11. Continuous Monitoring and Improvement

- ★ Track cybersecurity measurements and KPIs through continuous monitoring mechanisms.
- ★ Review and update the NIST CSF implementation as the organization's environment and threat landscape change

#12. Incident Response Planning

- ★ Create and record a NIST CSF-aligned incident response strategy.
- ★ Regular drills and exercises test the incident response plan

#13. Documentation and Reporting

- ★ Thoroughly document the NIST CSF implementation process.
- ★ Keep stakeholders informed of the company's cybersecurity progress.

#14. External Collaboration

- To improve cybersecurity procedures, collaborate with external partners, vendors, and industry peers
- Join threat intelligence and information-sharing programs.

#15. Audit and Compliance

- Assess NIST CSF and applicable regulatory compliance through periodic audits.
- Fix non-compliance concerns immediately.

16. Review and Adapt

- Regularly assess NIST CSF implementation effectiveness.
- Adjust the implementation plan based on lessons learned, threats, and organizational changes.