

NIST CSF CHECKLIST

1 – SCOPE

- Identify the people, processes, and technology that support your business

2 – GAP ANALYSIS

- Identify your current documentation posture
 - Have you specified and properly documented the activities and procedures that make up your company's control environment?
 - Do you review documents on a regular basis to make sure they are up to date and accurate?
- Identify your current control environment posture
 - What is the organization's governance structure?
 - What are the executive leadership and management tone and example?
 - Have you designed and implemented hiring and exit procedures?
 - What are the executive leadership and management tone and example?
 - How are personnel who are implementing or directing internal controls evaluated for competency?
 - Are possible threats being identified?
 - Have you put any mitigating plans in place?
 - Do you have a protocol for dealing with incidents and a disaster recovery plan in place?
 - What kind of management supervision and governance do you have in place for your control the environment and reporting events, security problems, and fraud?
- Identify your current security environment posture
 - Do you have access limited to positions that need it, with the appropriateness of the access? given being reviewed on a regular basis?
 - Do you have policies in place for giving and taking away access from workers, customers, and other parties?
 - Do you encrypt data while it's in transit and while it's at rest?
 - Do you impose restrictions on administrative access to the technological stack?
- Identify your current risk mitigation environment posture
 - Have you conducted vulnerability assessments or penetration testing regular basis to detect weaknesses in your environment?
 - Do you have backup processes in place?
 - Do you test your disaster recovery procedures on a yearly basis to guarantee that you can restart operations in case of a calamity?
 - Do you regularly check for intrusion attempts, system performance, and availability?
- Identify your current system changes environment posture

- Are system modifications tested and authorized before they are implemented?
- Do you inform your employees about system changes?
- Are your controls being monitored on a regular basis?
- Have you enabled notification of settings changes?
- Is your technology up to date in terms of upgrades?
- Do you have a system in place for separating development and production tasks?
- Identify your current remote working environment posture
 - Is technology being used uniformly across all employee locations?
 - Do you provide staff with regular security awareness training, address data privacy in common spaces, use secure connections while working from home, and raise awareness of phishing attempts?
 - Do you use multifactor authentication to get into your company's network and other systems?
 - Have you deployed mobile device management to make sure that mobile devices are encrypted and authenticated?

3 – PLANS OF ACTIONS AND MILESTONES (POAMs)

- Document your POAMs based on your gap assessment

4 – CONTROL IMPLEMENTATION

- Design the controls to address your gaps
- Implement controls to address your gaps
- Test the controls to ensure that they are operating effectively.

5 – SELF – ATTEST READY

- Identify the internal auditor
- Initiate kick-off to set expectations
- Grant them access to TrustCloud
- Self-Attest via TrustCloud

6 – MAINTENANCE

- Maintain the program to show continuous compliance via TC integrations